



BIGFOOTINTERACTIVE™

**Before the
FEDERAL TRADE COMMISSION
Washington, D.C. 20580**

**COMMENTS
Of
BIGFOOT INTERACTIVE, INC.
On the
CAN-SPAM Act Rulemaking, Project No. R411008**

Al DiGuido
Chief Executive Officer
Bigfoot Interactive, Inc.
315 Park Ave. South, 18th Floor
New York, NY 10010
212.995.7500

June 27, 2005

I. Introduction, Summary, and Background

Bigfoot Interactive, Inc. ("Bigfoot Interactive") is pleased to submit these comments in response to the Federal Trade Commission's ("Commission") request for public comment on the "CAN-SPAM Act Rulemaking, Project No. R411008." We appreciate the Commission's efforts to clarify the CAN-SPAM Act through this NPRM. Attached to these comments is a paper entitled "Email and Spam: Consumer Attitudes and Behaviors," which reports the results of a nationwide consumer survey conducted by Bigfoot Interactive and NOP World/Roper ASW in February 2005 (hereinafter "Bigfoot Interactive/RoperASW survey"). This paper provides an overview of current consumer perceptions and behaviors associated with email and spam, and will help provide context and perspective for some of our comments.

As the leading provider of email communications solutions and marketing automation technologies to the Fortune 2000, Bigfoot Interactive (www.bigfootinteractive.com) and its clients have a major stake in the success of legitimate commercial email communications. Bigfoot Interactive plays a leadership role in the industry, including active involvement in trade associations including the Direct Marketing Association (Ethics Policy Committee, Interactive Marketing Advisory Board, and the Council for Responsible Email), the Messaging Anti-Abuse Working Group, and the Email Service Provider Coalition. In addition, Bigfoot Interactive is a founding organizer and on the Steering Committee of the upcoming industry Email Authentication Implementation Summit.

Bigfoot Interactive supports the CAN-SPAM Act because it believes it is helpful in a multi-faceted approach to combating spam, which interferes with the delivery and effectiveness of legitimate email communications. Bigfoot Interactive believes that the Act has empowered law enforcement and ISPs with the authority they need to go after spammers and fraudulent email practices, and it has been reported that federal and state governmental entities and ISPs have leveraged the Act to bring criminal and civil enforcement actions against spammers.

Bigfoot Interactive believes that enforcement of the Act, in combination with other aspects of a multi-faceted approach to combating spam, has proven effective at significantly reducing spam and improving the recipient/consumer email experience since its enactment. In particular, technological improvements in anti-spam filtering and the advancement of email authentication protocols have helped to make a significant dent in the problem.

According to the Bigfoot Interactive/ASW Roper survey, a majority of consumers, 57 percent, strongly/somewhat agreed that the amount of spam they have received over the past year has decreased, which is in-line with recent announcements from major ISPs. America Online, for example, reported "a banner-year in the fight against spam that has resulted in a more than 75 percent decline in junk email on the service in 2004, as defined by members' spam reports," (America Online press release, *America Online Announces Breakthroughs In Fight Against Spam*, December 27, 2004). Meanwhile, Microsoft noted that, "as a result of the growing adoption of SIDF [an authentication protocol] worldwide, Microsoft has found notable improvements in the accuracy of its SmartScreen filtering process," (Microsoft press release, *Sender ID Framework Demonstrates Positive Results for E-Mail Authentication*, March 2, 2005). In short, there



is ample evidence of a significantly improved email environment only a year and a half since the enactment of the CAN-SPAM Act.

Bigfoot Interactive believes that the CAN-SPAM Act is not intended to interfere with the sending of legitimate commercial email. Although Bigfoot Interactive supports many elements outlined in the Commission's NPRM, Bigfoot Interactive is concerned that there are instances where further clarity to the Act might be necessary to avoid the potential for unintended consequences and burdens on legitimate senders of commercial email and/or negatively impact the consumer/recipient email experience.

Specifically, Bigfoot Interactive requests that the Commission, in this Rulemaking, should:

- Provide further clarification on the criteria designating the sole "Sender" of a commercial email;
- Indicate an acceptable time frame for honoring opt-out requests of at least ten business days;
- Establish a time limit of no more than five years for maintaining opt-outs; and
- Maintain senders' ability for recipients to take other steps in addition to sending a reply email message or visiting a single Web page to submit a valid opt-out request.

II. Provide further clarification on the criteria designating the sole "Sender" of a commercial email.

As outlined in the NPRM, the Commission proposes three elements, any *one or more* of which would determine the sender in situations when more than one person's products or services are advertised or promoted in a single message:

- (1) the person controls the content of the message;
- (2) the person determines the email addresses to which such message is sent;
- (3) the person is identified in the "from" lines as the sender of the message.

However, the Commission proposes that an entity may be considered the sole sender *only in cases when no other seller may satisfy any of them*. Bigfoot Interactive is concerned that this caveat could potentially impose unnecessary compliance burdens on many law-abiding industry members.

Depending on what is meant by "controls the content" and "determines the email addresses to which such message is sent," it could become difficult to establish that only one of multiple parties involved in such a message is the sole sender. This is because in many commercial email messages that contain promotional content from multiple marketers, it is common for several if not all of the parties to exert at least some degree of control over the content, and at least to some extent determine the email addresses to which such email is sent.

Bigfoot Interactive is concerned, therefore, that without further clarification, many common commercial email campaigns could be interpreted to have multiple-senders, burdening both businesses and recipients/consumers with confusing, multiple and disparate opt-outs and disclosures.

1. Bigfoot Interactive Proposes Alternative for Determining the Sole “Sender” in Messaging Where Multiple Marketers Are Present.

Bigfoot Interactive would support an approach similar to the Commission’s Rule determining whether the primary purpose of a message is commercial. Bigfoot Interactive proposes that:

Emails that include content from multiple marketers could be structured to have a single sender if:

- (1) the recipient reasonably would interpret from the “From” and/or subject line that the email contains advertising/promotional content from a single, dominant marketer; or
- (2) a single, dominant marketer’s content appears substantially at the top of the message’s body content; or
- (3) creative elements such as color and graphics are used to emphasize a single, dominant marketer’s ownership of the message and sender obligations under CAN-SPAM relative to other marketers in the message.

III. Indicate an acceptable time frame for honoring opt-out requests of at least ten business days.

The Commission proposes shortening the time that a sender has to honor a recipient’s opt-out request from 10 to 3 business days. Bigfoot Interactive is concerned that this could cause significant challenges for many legitimate marketers, especially pertinent to larger, structurally complex organizations. Bigfoot Interactive therefore requests that the Commission maintain at least the current ten business-day opt-out framework.

While there is no doubt that modern technology – including Bigfoot Interactive’s own email deployment platform – enables robust opt-out processing functionality, in many cases email service providers are only responsible for managing specific messaging streams and/or campaigns for their clients, leaving marketer data processes and interaction between global infrastructure, divisions, affiliates, partners and systems much more relevant to a company’s ability to verify that an email has been removed from all required databases within a certain timeframe. This can become even more complicated when taking into account corporate mergers and acquisitions where disparate legacy database systems must process opt-outs against one another.

Bigfoot Interactive further points out:

1. No Record of Abuse.

As the Commission itself noted in the NPRM, the record to-date does not reflect abuse of the current ten-day opt-out framework. According to the Commission “the record does not demonstrate whether fears of ‘mail-bombing’ are well founded.”

2. Record of Enforcement Progress, Technological Advances and Increased Recipient/Consumer Control of the Inbox.

As highlighted in the introduction of our comments, the record to-date reflects substantial progress in diminishing spam and also that consumers are demonstrating increased control over their inboxes since the enactment of the CAN-SPAM Act. The Commission itself noted in its NPRM that, “the purpose of the opt-out provision in the CAN-SPAM Act is to protect recipients from unwanted commercial email.” Bigfoot Interactive believes this is already occurring under the existing 10-day opt-out framework, and without placing unnecessary burdens on the legitimate business community.

Enforcement of the Act combined with technological advances continues to yield significant results, and the market continues to make great strides on its own to protect consumers and enhance the growth, safety and promise of email as a vehicle for global commerce, communication and education.

In particular, Bigfoot Interactive highlights that ongoing advancements such as the implementation of ISP “whitelists,” more advanced email authentication, accreditation and reputation solutions, ISP “self-containment,” and the incorporation of end-recipient/consumer feedback via integrated, easy-to-use spam complaint buttons in ISP’s graphical user interfaces has resulted in powerful market-based incentives for legitimate marketers to maintain consumer-centric values and accommodate recipient/consumer communication preferences. Meanwhile, these technological advances have also been highly effective at identifying and blocking egregious spammers.

To ensure legitimate high-volume email delivery, marketers are increasingly required to apply for ISP “whitelists” and maintain complaint rates estimated to be less than 0.1 percent in some cases. Furthermore, ISPs increasingly are instituting “feedback loops” to share complaints with whitelisted senders and other ISPs so that they can unsubscribe complainants from their lists and also in order to assist them in identifying problematic, high-complaint messaging streams emanating from their IP addresses/computer networks so they can implement corrective measures. This has helped make significant contributions to the overall decline in spam.

According to the Bigfoot Interactive/RoperASW survey, consumers strongly correlate using spam complaint buttons with inbox control. Of the 23 percent of consumers that reported having recently used a spam complaint button, 72 percent strongly/somewhat agreed with the statement “I have decreased the frequency of having to report spam” with another 68 percent strongly/somewhat agreeing that “Since using the ‘This is Spam’ or ‘Report Spam’ button, the amount of unsolicited email I received has decreased.”

Simply put, exceeding miniscule ISP complaint thresholds is playing an increasing role in email delivery and blockage. Therefore, email delivery is largely being regulated by the market and consumers themselves, and without interfering with the normal flow and continued growth of legitimate ecommerce.

3. *Potential for Unintended Consequences.*

Law abiding companies will always refrain from sending further email until the opt-out is verified within a legally mandated time period. Because of this, moving

to three days could result in the unintended inhibition of legitimate commercial email communications for many law-abiding companies. For example, a company that currently communicates with its customers even only once a week would have to refrain from emailing *all* of its customers on such a schedule if it is unable to verify the complete erasure of an opt-out requested email address across organizationally complex database infrastructure and systems within a three day timeframe. The end result for some organizations could be that a majority of customers that *haven't* opted-out and have even *requested* regular commercial communications will be prevented from receiving them. This will result in the inhibition of legitimate ecommerce.

Bigfoot Interactive therefore requests the Commission reconsider its proposal to shorten the timeframe for processing opt-outs to three days, or in the very least, that the Commission should revisit this issue in a few years from now.

Bigfoot Interactive believes that at least the ten business day timeframe should be maintained because the record reflects that significant progress has been made in protecting consumers from spam with this framework in place, accompanied by the steady and healthy growth of legitimate email marketing. The Direct Marketing Association (DMA) estimates that legitimate commercial email resulted in approximately \$39 billion in sales in 2004, including about \$9 billion in small business sales (DMA press release, *The DMA Co-Underwrites Email Authentication Implementation Summit 2005*, May 11, 2005). This represents solid year-over-year growth compared to the DMA's estimate of the size of the legitimate email marketing sales in 2003, which was approximately \$33 billion (DMA press release, *DMA Submits Comments to FTC on Do-Not-Email List Proposal*, March 31, 2004). We must ensure that legitimate commercial email is protected to the continued benefit of the American economy. Bigfoot Interactive believes that shortening the opt-out timeframe to 3 days would do little in terms of further protecting consumers from spam while inflicting harm on the burgeoning legitimate commercial email marketplace.

IV. Establish a time limit of no more than five years for maintaining opt-outs;

The Commission indicated in the NPRM that it has determined not to propose a time limit on the duration of an opt-out. Bigfoot Interactive requests that the Commission reconsider this position, because individuals change email addresses regularly, and there are hard costs associated with the ongoing suppression of email addresses. Law-abiding marketers should not have to indefinitely suppress email addresses, especially those that become non-functional or reassigned to new individuals over time. Limiting the duration to under five years would reduce expenses and also will help ensure that individuals who are reassigned email addresses will not unknowingly be opted-out of receiving commercial email. Recipients/consumers with functional email addresses that are added back to marketers' lists after a five-year or other established timeframe could simply re-exercise their right to opt-out.

1. Bigfoot Interactive research indicates that substantial email address turnover/"churn."

The Bigfoot Interactive/RoperASW survey revealed that 22 percent said they have switched their ISP email account (13 percent) or are considering switching accounts (9 percent) over a one-year period. This rate of email churn indicates

that for most marketers, the majority of in-house suppression lists will likely be composed of non-functional email addresses *within less than five years*.

Furthermore, of this pool, the primary reason for switching or considering switching email accounts came down to cost/price (34 percent), followed by those that cited an upgrade to broadband/high speed services (25 percent). These reasons point to continued volatility and intense competition in the ISP marketplace, a trend that Bigfoot Interactive anticipates will continue into the foreseeable future. In addition, these reasons compare to only 3 percent of consumers who report switching or considering switching their accounts due to receiving too much spam or poor anti-spam functionality and features – a further sign of progress in diminishing spam.

V. Maintain senders' ability for recipients to take other steps in addition to sending a reply email message or visiting a single Web page to submit a valid opt-out request.

The Commission proposes that senders should not be able to require that recipients take steps other than sending a reply email or visiting a single Internet web page to submit a valid opt-out request. Bigfoot Interactive supports that recipients must always be provided a simple and free, Internet-based opt-out mechanism.

However, marketers and recipients/consumers need flexibility in terms of how they verify the legitimacy of opt-outs, so that recipients are not unknowingly opted-out of messages by others. In some cases, visiting a single web page may not be sufficient. For example, in an age of malicious software attacks targeted at ecommerce companies, some marketers might ask an individual to perform a simple challenge that only humans can accomplish before opting them out. Other marketers might ask that recipients/consumers to enter their email address to be opted-out on one web page, and then provide confirming information sent back to that address on another web page. Allowing a degree of flexibility in effectuating opt-outs would therefore provide protections to both businesses and consumers alike. Bigfoot Interactive suggests that a more appropriate standard would be that marketers must always offer a simple, cost-free and effective Internet-based opt-out mechanism.

VI. Conclusion

Bigfoot Interactive appreciates this opportunity to comment on the important issues raised in the NPRM. We welcome the opportunity to work with the Commission as it issues its proposed rules.

Respectfully submitted,

Al DiGuido
Bigfoot Interactive, Inc.



BIGFOOTINTERACTIVE™

EMAIL AND SPAM: CONSUMER ATTITUDES AND BEHAVIORS

Bigfoot Interactive / NOP World/Roper ASW, February 2005

FEBRUARY 2005

Michael Della Penna
Chief Marketing Officer
mdellapenna@bigfootinteractive.com





Table of Contents

BACKGROUND & METHODOLOGY..... 1

EXECUTIVE SUMMARY 2

DATA FINDINGS 4

 Active Accounts 4

 Software Used To Read Email 5

 ISP/Email Clients - Customer Loyalty 6

 ISP/Email Client - Dissatisfaction 7

 Report Spam 8

 Decrease In Volume Of Spam 9

 Decrease In Volume Of Spam 10

 Relevance Up 11

 Anti-Spam Software Use Up 12

 False Positive Issue Continues 13

 Add To Address Book Effective 14

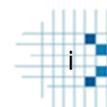
 Phishing 15

 Spyware 16

 Consumers Want More Help 17

APPENDIX: QUESTIONNAIRE

© 2005 Bigfoot Interactive, Inc. Confidential. Circulation or disclosure in whole or in part of this report outside the authorized recipient organization is expressly forbidden without the prior written permission of Bigfoot Interactive, Inc. Bigfoot Interactive and DREAM are trademarks of Bigfoot Interactive, Inc. All other trademarks are the property of their respective companies. Information is based on best available resources. Opinions reflect judgment at the time and are subject to change.





BACKGROUND & METHODOLOGY

RoperASW was commissioned by Bigfoot Interactive to conduct a study among a nationally representative sample of adults 18 years or older, who have Internet access at home. The study was conducted to determine the consumer level of satisfaction with current email software, as well as their handling of unsolicited emails and email blocking features. The study also focused on consumer perceptions in the areas of email relevancy, the effectiveness of adding legitimate senders to their address books and how consumers handle the threat of spyware and fraudulent phishing emails.

Data for this study was gathered via telephone through RoperASW's weekly *OmniTel* study. The sample for each week's *OmniTel* wave consisted of 1,004 completed interviews, comprised of male and female adults (in approximately equal number), 18 years of age or older. Each *OmniTel* study is based on a random digit dialing (RDD) probability sample of all telephone households in the continental United States. The RDD sampling system provides an equal probability of selecting listed and unlisted phones in their proper proportions.

The results contained in this report are based on interviews conducted from February 18-20, 2005. A total of 537 interviews were completed among adults 18 years or older with Internet access at home (260 with female adults and 277 with male adults).



EXECUTIVE SUMMARY

Leading ISPs And Email Clients:

Of those surveyed, close to half of the **respondents (45%) indicated the use of 2 or more email accounts at home**, with a mean of 2.5 accounts. Adults with Internet access at home use a variety of ISPs or Email Clients/Tools. Among the leading brands/products used to read email were AOL, (20%), Yahoo (19%) and Outlook Net (19%). It seems that Yahoo's free offering and powerful brand name and Outlook's ability to port multiple email accounts into one interface have helped accelerate their popularity as either the primary or secondary email account. Interestingly, if Outlook, Hotmail and MSN users are combined, Microsoft boasts 47% of the market among consumers surveyed. In an effort to maintain market share, AOL recently announced plans to offer a free Web Mail service for non-subscribers.

Continued Volatility:

More than 13% of respondents indicated they have switched ISPs or Email Clients/Tools in the past six months. In addition, 9% are considering switching in the next 6 months. Cost and **the rapid adoption of broadband appears to be having substantial consequences for the competitive ISP/Email Client marketplace**. Of those consumers who said they switched or considered switching their email account(s) in the last year, a majority said they did so because of cost (34%) or upgrading to broadband services (25%), with a mere 3 percent saying they did so because they received too much spam.

SPAM:

2005 marks a turning point in the war on spam. The emergence of anti-spam efforts seems to be increasing awareness as well as the use/perceived use of these tools. For the first time in several years, research indicates that a majority of those surveyed (57%) agreed they are receiving less spam in the inbox than they did one year ago. In addition, more than 65% of consumers surveyed stated they were currently using anti-spam filtering or challenge response software. Furthermore, ISP's and Email Clients/Tool's efforts to identify and stop spam at the gateway have also been effective. In-line with these findings, America Online recently announced that they have experienced a substantial annual reduction in spam received both at the gateway as well as that reported by their members.

Relevancy Rises:

More consumers consider legitimate communications more relevant today than they were one year ago. More than half of respondents (53%) agreed that email they receive is usually targeted to their need and interests, and 57% agreed that the email communications they receive from companies they do business with are more targeted/relevant than the communications they received from those same companies last year. Increasingly, email that is irrelevant to consumers is being tagged as spam and legitimate marketers continue to



improve and fine-tune their email communication efforts around individual consumer needs, preferences and interests. The concept of one size fits all, regardless of the medium is no longer acceptable as consumers become more sensitive to message bombardment.

False Positive Issues Persist:

While progress has been made on multiple levels in the fight against spam, the proliferation of new anti-spam and challenge response products/services continue to unfortunately generate false positives. Roughly a third of consumers (32%) agreed that email they have requested from a trusted source has been delivered to a junk mail folder. In addition, a quarter of consumers agreed they recently have lost or did not receive an email that they were supposed to receive from a trusted source. Clearly, we must continue to work collaboratively with all key stakeholders to protect legitimate email communications from anti-spam filtering and false positives.

Add To Address Book Awareness Grows:

Consumers are increasingly looking to take control of their inboxes, and are doing so almost as much to ensure the delivery of wanted communications as to block spam. Over half (56%) agreed that they always add trusted, legitimate senders to their address books, while 65% agreed that they are currently using anti-spam filtering or challenge response software. However, marketers can be doing more to educate consumers as less than half (42%) agreed legitimate emails they subscribed to encouraged them to add the company to their address book at the time of subscription or on each message received. Furthermore, only half of consumers surveyed (55%) routinely check their spam/junk folder for legitimate messages. Clearly, we must continue to work collaboratively with all key stakeholders to protect legitimate email communications from anti-spam filtering and false positives.

Security And Fraud Concerns:

Internet security threats like phishing and spyware have begun to overshadow concerns about spam. About a third of respondents (34%) said they have received a phishing email, and more than half (55%) believed their computer has been infected by spyware. An overwhelming 82% agreed that they are concerned about spyware and the threat it poses to their online security. In addition, only 32% of consumers surveyed agreed they were confident they could identify or detect a fraudulent/phishing email designed to look like those of legitimate businesses or financial institutions.

DATA FINDINGS

Active Accounts

Please tell me the number of active accounts you have personally at home.

Close to half of **respondents (45%)** indicated the use of **2 or more email accounts**. On average respondents reported 2.5 active accounts.

Number of Active Accounts

Base: Internet Access At Home	Total (610) %	Male (314) %	Female (296) %
None (net)	12	12	12
One Or More (net)	88	88	88
1	43	41	45
2	23	21	25
3	12	12	11
4	3	4	2
5	3	4	3
6 or more	4	6	2
Mean excluding zero	2.5	3	2

*Numbers are rounded

Software Used To Read Email

Please indicate what email tool, software or client you use to read your email.

58% of consumers surveyed said they use AOL (20%), Yahoo! (19%) and Outlook Express/Outlook Other (19%) to read their email. Combining Outlook Express (15%) and Outlook Other (4%) brings Outlook's total share to 19%.)

Microsoft's Hotmail (12%) and MSN (9%) comprise 21% of consumers using both to read their mail along with Internet Explorer (3%) and Microsoft (3%) being cited which amounts to 27%. Interestingly, if Outlook Express/Outlook Other are combined with this total, Microsoft boasts 47% of the market surveyed.

Software Used to Read Email

Base: Having One Or More Email Accounts	Total (537) %	Male (277) %	Female (260) %
Any (net)	92	92	93
AOL	20	18	22
Yahoo!	19	19	20
Outlook Express	15	16	13
Hotmail	12	12	12
MSN	9	8	9
Outlook Other	4	6	2
Earthlink	3	3	4
Internet Explorer	3	2	4
Microsoft	3	5	1
Cable Provider Interface	3	3	3
DSL Provider Interface	2	1	3
Road Runner	2	2	1
School	2	1	3
Netscape	2	1	1
United Online/Juno/NetZero	1	.2	2
Thunderbird	1	1	.2
Web Mail	1	.4	1
Gmail	1	1	.4
AT&T Worldnet	.1	0	.3
Other	10	9	11
None	1	1	1
Don't Know/No Response	7	7	6

ISP/Email Clients - Customer Loyalty

Please tell me if you have switched Internet Service Providers or Email Service Providers you use to read email in the last 6 months or are considering switching providers in the next 6 months.

Most adults with a primary service provider (72%) have not switched providers in the last six months or considered switching providers in the next six months. This indicates increased short-term loyalty.

However, 22% of adults surveyed said they have switched providers (13%) or are considering switching providers (9%) over a one-year period.

ISP/Email Clients - Customer Loyalty

Base: Having One Or More Email Accounts	Total (537) %	Male (277) %	Female (260) %
Switched Providers in the Last Six Months	13	11	15
Considered Switching Providers in the Next Six Months	9	10	7
Neither	72	72	71
I Don't Make This Kind of Decision	6	6	5
Don't Know/No Response	2	1	2

*Numbers are rounded

ISP/Email Client - Dissatisfaction

Please tell me your primary reason for switching or considering switching email clients or accounts.

Out of the 537 adults surveyed, 115 (58 males & 57 females) answered that the primary reason for switching or considering switching email clients or accounts came down to Cost/Price (34%), followed by those that cited an Upgrade to Broadband/High Speed Services (25%).

It is interesting to note that there was a noticeable difference in the weight given to these answers among male and female respondents. Female respondents placed more emphasis on Cost/Price (38%) vs. male adults (30%). The second highest response showed that male respondents cited an Upgrade to Broadband/High Speed Services (37%) vs. (12%) of female respondents. Usability Issues ranked third (15%) for reasons given for switching or considering making a switch in providers.

ISP/Email Client Dissatisfaction

Base: Switched Providers In The Last 6 Months/Considering To Switch Providers In The Next 6 Months	Total (115) %	Male (58) %	Female (57) %
Cost/Price	34	30	38
Upgrade to Broadband/High Speed Services (Cable/DSL)	25	37	12
Usability Issues - Poor Features/Functionality	15	13	16
Customer Service Problems or Issues	6	4	8
Moved	5	5	6
Too Much Spam or Poor Anti-Spam Features/Functionality	3	2	5
Computer/Software Upgrade	2	2	2
Storage Capacity Issues/Limits	2	0	4
Other	9	7	10
Don't Know/No Response	1	1	0

*Numbers are rounded



Report Spam

Have you used the “Report Spam” or “This is Spam” button or link?

Approximately a quarter (23%) of respondents indicated use of the “Report Spam” or “This is Spam” button or link.

Used “Report Spam” Or “This Is Spam” Button Or Link

Base: Having One Or More Email Accounts	Total (537) %	Male (277) %	Female (260) %
Yes	23	22	25
No	74	76	72
Don't Know/No Response	3	2	3

*Numbers are rounded

Decrease In Volume Of Spam

Adults with Internet access at home were read a series of statements and then asked their level of agreement with each. Overall, out of the 537 consumers surveyed, 57% Agreed the amount of spam they have received over the last year has decreased.

Base: Having One Or More Email Accounts	Total (537) %	Male (277) %	Female (260) %
The amount of spam I have received over the past year has decreased.			
Strongly/Somewhat Agree (Net)	57	59	55
Somewhat/Strongly Disagree (Net)	39	37	41
Don't Know/No Response	4	4	4

*Numbers are rounded

Decrease In Volume Of Spam

Out of the 537 adults surveyed, 126 (61 males & 64 females) answered that they have used the “Report Spam” or “This is Spam” Button or Link.

72% of consumers who have used the “Report Spam” or “This Is Spam” Button or Link Strongly/Somewhat Agreed they have decreased the frequency of having to report spam. 68% Strongly/Somewhat Agreed they have seen a decrease in the amount of unsolicited email.

Base: Used “Report Spam” Or “This Is Spam” Button Or Link	Total (126) %	Male (61) %	Female (64) %
Since using the “This is Spam” or “Report Spam” button, the amount of unsolicited email I received has decreased.			
Strongly/Somewhat Agree (Net)	68	70	66
Somewhat/Strongly Disagree (Net)	29	29	29
Don’t Know/No Response	3	1	5
I have decreased the frequency of having to report spam.			
Strongly/Somewhat Agree (Net)	72	78	66
Somewhat/Strongly Disagree (Net)	23	18	29
Don’t Know/No Response	5	4	5
When clicking on the “Report Spam” or “This is Spam” button I am unsubscribing from the email			
Strongly/Somewhat Agree (Net)	49	34	64
Somewhat/Strongly Disagree (Net)	44	65	23
Don’t Know/No Response	7	1	13

*Numbers are rounded

Relevance Up

Respondents were asked two questions related to relevancy of their email communications and their perception of it over the past year from companies that have conducted business with them.

Over half of consumers surveyed, 53% Strongly/Somewhat Agreed when asked if email they receive is usually targeted to their needs and interests.

This number increased to 57% that Strongly/Somewhat Agreed when asked if the email communications they receive from companies they do business with are more targeted/relevant than the same communications they received from the same companies last year.

Base: Having One Or More Email Accounts	Total (537) %	Male (277) %	Female (260) %
Email I receive is usually targeted to my needs and interests.			
Strongly/Somewhat Agree (Net)	53	49	58
Somewhat/Strongly Disagree (Net)	46	51	42
Don't Know/No Response	1	1	1
In general, I would say that email communications I receive from companies I do business with are more targeted/relevant than the same communications I got from the same companies last year.			
Strongly/Somewhat Agree (Net)	57	56	58
Somewhat/Strongly Disagree (Net)	35	34	36
Don't Know/No Response	8	10	6

*Numbers are rounded

Anti-Spam Software Use Up

The majority of consumers, 65% Strongly/Somewhat Agreed they are currently using anti-spam filtering or challenge response software. Approximately half of adults surveyed Strongly Agreed with this statement.

This level of agreement coincides with the response given by consumers that spam has decreased over the past year since there has been a rise in the use of anti-spam software. 72% of consumers Strongly/Somewhat Agreed that they have decreased the frequency of having to report spam.

Base: Having One Or More Email Accounts	Total (537) %	Male (277) %	Female (260) %
I am currently using anti-spam filtering or challenge response software.			
Strongly/Somewhat Agree (Net)	65	67	63
Somewhat/Strongly Disagree (Net)	30	28	32
Don't Know/No Response	5	5	5

*Numbers are rounded

False Positive Issue Continues

Slightly over half, 52% of consumers Strongly/Somewhat Agreed that they routinely check their spam/junk folder for legitimate messages. Women were more likely than men to agree they routinely check their spam/junk folder.

These figures were substantiated by 32% of consumers that Strongly/Somewhat Agreed that email they have requested from a trusted source was delivered to a junk mail folder. It was interesting to note that men Strongly/Somewhat Agreed 35% vs. 29% of women that email requested from a trusted source was delivered to a junk mail folder, but checked this folder less frequently than women did.

25% of consumers indicated Strongly/Somewhat that they have recently lost or did not receive an email that they were supposed to receive from a trusted source.

Base: Having One Or More Email Accounts	Total (537) %	Male (277) %	Female (260) %
I routinely check my spam/junk folder for legitimate messages.			
Strongly/Somewhat Agree (Net)	52	49	54
Somewhat/Strongly Disagree (Net)	45	47	43
Don't Know/No Response	3	4	3
Email I have requested from a trusted source was delivered to a junk mail folder.			
Strongly/Somewhat Agree (Net)	32	35	29
Somewhat/Strongly Disagree (Net)	63	60	66
Don't Know/No Response	5	5	4
I recently have lost or did not receive an email that I was supposed to receive from a trusted source (friend, family, company I have a relationship with).			
Strongly/Somewhat Agree (Net)	25	23	26
Somewhat/Strongly Disagree (Net)	72	72	72
Don't Know/No Response	4	5	2

*Numbers are rounded

Add To Address Book Effective

Over half, 56% of consumers Strongly/Somewhat Agreed that they always add legitimate, trusted senders to their address book. This figure represents the action taken by a large number of consumers in order to ensure the delivery of email communications from legitimate, trusted senders and not have it wind up in the spam/junk folder of their email account.

42% of consumers Strongly/Somewhat Agreed that legitimate email they subscribe to usually encourages them to add the company to the address book at the time of subscription or on each message. Marketers are adopting this best practice to ensure delivery of their email communications.

Base: Having One Or More Email Accounts	Total (537) %	Male (277) %	Female (260) %
I always add legitimate, trusted senders to my address book.			
Strongly/Somewhat Agree (Net)	56	56	56
Somewhat/Strongly Disagree (Net)	42	42	42
Don't Know/No Response	2	2	2
Legitimate emails I subscribe to usually encourage me to add the company to my address book at the time of subscription or on each message.			
Strongly/Somewhat Agree (Net)	42	43	41
Somewhat/Strongly Disagree (Net)	54	51	57
Don't Know/No Response	4	6	3

*Numbers are rounded

Phishing

Less than half of consumers, 34% Strongly/Somewhat Agreed they have received a fraudulent or phishing email. These emails were disguised as a legitimate business correspondence that asked them to verify personally identifiable information (PII) such as a credit card or social security number on their account. This information can be used for criminal activity such as identity theft.

Over half of the consumers surveyed, 64% Strongly/Somewhat Agreed that they are confident they can identify or detect a fraudulent/phishing email designed to look like those of legitimate businesses, financial institutions, & government agencies.

Base: Having One Or More Email Accounts	Total (537) %	Male (277) %	Female (260) %
I have recently received a fraudulent or “phishing” email which was disguised as a legitimate business correspondence that asked me to verify personal information such as a credit card/ss # or password on my account which can be used for criminal activity such as identity theft.			
Strongly/Somewhat Agree (Net)	34	36	32
Somewhat/Strongly Disagree (Net)	63	62	65
Don't Know/No Response	2	2	3
I am confident I can identify or detect a fraudulent, “phishing” email that is designed to look like those of legitimate businesses, financial institutions, and government agencies.			
Strongly/Somewhat Agree (Net)	64	66	63
Somewhat/Strongly Disagree (Net)	33	33	34
Don't Know/No Response	2	2	3

*Numbers are rounded

Spyware

The majority of consumers surveyed, 82% Strongly/Somewhat Agreed they are concerned about spyware and the threat it causes to their online privacy.

Over half of consumers, 55% Strongly/Somewhat Agreed they have been infected with spyware that caused pop-up ads on their computer, hijacked their browser start page and altered important system files. Interestingly, men are more likely than women (61% vs. 49%) to agree that their computer has been infected with spyware.

Base: Having One Or More Email Accounts	Total (537) %	Male (277) %	Female (260) %
I am concerned about spyware and the threat it causes to my online privacy.			
Strongly/Somewhat Agree (Net)	82	82	81
Somewhat/Strongly Disagree (Net)	16	15	17
Don't Know/No Response	2	3	2
I have been infected with spyware that caused pop-up ads on my computer, hijacked my browser start page or pages, and altered important system files.			
Strongly/Somewhat Agree (Net)	55	61	49
Somewhat/Strongly Disagree (Net)	42	36	49
Don't Know/No Response	3	4	2

*Numbers are rounded

Consumers Want More Help

Consumers are looking for more help in the areas of authentication/accreditation, ISP/Email Clients unsubscribe option for email lists, and additional security features embedded within their email communications.

There was a large majority of consumers, 89% that Strongly/Somewhat agreed they would like their ISP/Email Client to include an icon to indicate email has been authenticated and is from a legitimate/trusted sender.

There was a majority of consumers, 86% that Strongly/Somewhat Agreed they would like their ISP to include an unsubscribe option that would safely remove them from email lists.

42% of consumers Strongly/Somewhat Agreed they would be interested in having their credit card company add a unique feature such as the last 4 digits of their credit card on every message to ensure that the email is legitimate.

Base: Having One Or More Email Accounts	Total (537) %	Male (277) %	Female (260) %
I would like my ISP/Email client to include an icon to indicate email has been authenticated and is from a legitimate/trusted sender.			
Strongly/Somewhat Agree (Net)	89	87	90
Somewhat/Strongly Disagree (Net)	10	11	9
Don't Know/No Response	2	2	1
I would prefer if my ISP or ESP would include an unsubscribe option that would safely remove me from email lists.			
Strongly/Somewhat Agree (Net)	86	86	86
Somewhat/Strongly Disagree (Net)	12	12	12
Don't Know/No Response	2	2	2

*Numbers are rounded

However, interest in credit card validation techniques commonly used in email is mixed. The majority of consumers (54%) were not interested in including the last four digits of their credit card on every message to validate the email message is legitimate.

Base: Having One Or More Email Accounts	Total (537) %	Male (277) %	Female (260) %
I would be interested to have my credit card company add a unique feature such as the last 4 digits of my credit card on every message to validate the email message is legitimate			
Strongly/Somewhat Agree (Net)	42	44	41
Somewhat/Strongly Disagree (Net)	54	52	56
Don't Know/No Response	4	5	3

*Numbers are rounded

APPENDIX: QUESTIONNAIRE

EMAIL3

OMT-0508

**ASK AMONG THOSE WITH INTERNET ACCESS AT HOME,
[CASH Q. 2 (4,23)]**

1. Please tell me the number of active email accounts you have personally at home? (RECORD NUMBER.)

**IF "0" IN Q. 1, SKIP TO NEXT SECTION.
ALL OTHERS CONTINUE.**

2. Please indicate what email tool, software or client you use to read your email (DO NOT READ LIST. CHECK AS MANY AS APPLY)

Earthlink	1
AOL	2
MSN	3
United Online/Juno/Netzero	4
AT&T Worldnet	5
Hotmail	6
Yahoo!	7
Gmail	8
Outlook Express	9
Outlook Other	10
DSL Provider Interface	11
Cable Provider Interface	12
Other (Specify:)	13
None	null
Don't Know	dk

3. Please tell me if you have switched Internet Service Providers or Email Service Providers you use to read email in the last 6 months or are considering switching providers in the next 6 months. (DO NOT READ LIST. CHECK AS MANY AS APPLY.)

Switched Providers in the last Six Months	1	}	(CONTINUE)
Considering Switching Providers in the Next Six Months	2		
Neither	3	}	(SKIP TO Q. 4a)
I don't make this kind of decision	4		
Don't know	dk		

4. Please tell me your primary reason for switching or considering switching email clients or accounts. (DO NOT READ LIST. CHECK ONLY ONE RESPONSE.)

Usability issues- Poor features/functionality	1
Storage Capacity issues/limits	2
Computer/Software Upgrade	3
Too much spam or poor anti-spam features/functionality	4
Customer service problems or issues	5
Upgrade to broadband/high speed services (Cable/DSL)	6
Cost/price	7
Other (Specify:)	8
Don't know	dk

- 4a. Have you used Report Spam or This is Spam Button or Link?

Yes	1	(CONTINUE)
No	2	} (SKIP TO Q. 5.4)
Don't know	dk	

5. Now, I'd like to read you several statements. For each one please tell me how much you agree or disagree. Would you say you agree strongly, agree somewhat, disagree somewhat or disagree strongly? Let's start with. . . (READ LIST. ROTATE. CHECK ONLY ONE RESPONSE FOR EACH.)

		<u>AGREE STRONGLY</u>	<u>AGREE SOMEWHAT</u>	<u>DISAGREE SOMEWHAT</u>	<u>DISAGREE STRONGLY</u>	<u>(DO NOT READ) DON'T KNOW</u>
(IF YES IN Q. 4a, I have ASK:)	Since using the "This is Spam" or "Report Spam" button, the amount of unsolicited email I have received has decreased.	1	2	3	4	dk
	decreased the frequency of having to report spam	1	2	3	4	dk
	When I click on the "This is spam" or "Report Spam" button I am unsubscribing from the email.	1	2	3	4	dk
	The amount of spam I have received over the past year has decreased.	1	2	3	4	dk
	I recently have lost or did not receive an email that I was suppose to receive from a trusted source (Friend, Family, company I have relationship with)	1	2	3	4	dk
	Email I have requested from a trusted source was delivered to a junk mail folder.	1	2	3	4	dk
	I would prefer if my Internet Service Provider or Email Service Provider would include an unsubscribe option that would safely remove me from email lists	1	2	3	4	dk
	I have recently received a fraudulent or "phishing" email which was disguised as a legitimate business correspondence that asked me to verify personal information such as a credit card or social security number or password on my account which can be used for criminal activity such as identity theft.	1	2	3	4	dk
I am confident I can identify or detect a Fraudulent, "phishing" Email that is designed to look like those of legitimate businesses, financial institutions, and government agencies.	1	2	3	4	dk	

(GRID CONTINUED ON NEXT PAGE)

	<u>AGREE STRONGLY</u>	<u>AGREE SOMEWHAT</u>	<u>DISAGREE SOMEWHAT</u>	<u>DISAGREE STRONGLY</u>	<u>(DO NOT READ) DON'T KNOW</u>
I would like my Internet Service Provider /Email client to include an ICON to indicate email has been authenticated and is from a legitimate/trusted sender.	1	2	3	4	dk
I would be interested to have my Credit Card company add a unique feature such as the last 4 digits of my credit card on every message to validate the email message is legitimate.	1	2	3	4	dk
I routinely check my spam/junk folder for legitimate messages.	1	2	3	4	dk
I always add legitimate, trusted senders to My address book.	1	2	3	4	dk
Legitimate emails I subscribe to usually encourage me to add the company to my address book at the time of subscription or on each message	1	2	3	4	dk
Email I receive is usually targeted to my needs and interests.	1	2	3	4	dk
In general, I would say that email communications I receive from companies I do business with are more targeted/relevant than the same communications I got from the same companies last year.	1	2	3	4	dk
I am currently using anti-spam filtering or challenge response software. 1	2	3	4	dk	
I have been infected with spyware that caused pop-up ads on my computer, hijacked my browser start page or pages, and altered important system files	1	2	3	4	dk
I am concerned about spyware and The threat it causes to my online privacy	1	2	3	4	dk