A Look at Consumers' Awareness of Email Security and Practices

or

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

Part I

Note: This is Part 1 of two parts of the report. Part I includes the abstract, introduction, summary and analysis. Part 2 includes the detailed responses to the report with associated charts and graphics. The report was separated into two files to make downloads easier.

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

by

Insights Worldwide Research

A Look at Consumers' Awareness of Email Security and Practices

or

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

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

Note: This is part 1 of the report and includes the survey report abstract, introduction, summary and analysis. Part 2 of the report includes the detailed responses to the survey with associated charts and graphics. The report was split into two files for easier downloading.

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)

Survey Objectives

This survey was developed:

- To be a voice for consumers that will help ISPs, email providers and vendors better understand the issues their users are confronting with email
- To gauge the general level of consumers' awareness of spam issues and understand how they distinguish legitimate email from spam
- To gauge how open consumers are to network operators' efforts to identify spam-creating bots on their home computers and to remove bots from their systems
- To generate a benchmark for future MAAWG research

Contributors

The MAAWG Consumer Survey Project Team, including MAAWG Senders Committee Co-Chair Dennis Dayman with Katrina Anderson, Christine Borgia, J.D. Falk, Tara Natanson and Laurie Jill Wood, were instrumental in defining the survey objectives, developing the questionnaire, and overseeing the survey process. The MAAWG Senders Committee, MAAWG Collaboration Committee and the organization's Board of Directors also provided invaluable direction and support throughout this project.

Once the data was obtained, MAAWG solicited additional analysis and insights from Ferris Research, Inc., an independent industry analysis firm that has been covering developments in the email and messaging market for over 17 years. Ferris analysts David Ferris and Richi Jennings both added their perspectives and recommendations to this report based on the survey results.

II. Summary of the Findings

In order to understand consumer awareness and perceptions, Insights Worldwide Research conducted 800 interviews among general consumers across the United States and Canada. This included 400 interviews conducted by telephone and 400 conducted online. In all cases, the respondent was a general consumer and determined not to be an expert in Internet security or to only use an email address that was managed by a professional IT department within a business organization. A detailed description of the survey methodology is available in Appendix D.

Following is a summary of some significant results. A detailed report of the findings, including the response to each question, are included in Section V, "Detailed Findings."

A. Internet and Email Usage

- Although not security "experts," two-thirds of all respondents indicated they are very or somewhat experienced with Internet security. Respondents who said they were Internet security experts were excluded from this research.
- The majority of respondents have an email at home, or both at home and at work. Just 2% say their email address is at work only.
- When asked what is most important to them in sending and receiving email, personal email from friends and family is most important, followed by receipts and/or shipping details, and notifications from banks and creditors falls into third place. Other types of emails, newsletters and marketing materials fall into the final tier.

B. Action Against Spam

- Most respondents install a filter in order to avoid spam. Approximately one-third avoid posting or releasing their email address, and approximately one-fourth use separate emails for situations they think might generate spam.
- About 21% take no action to prevent receiving spam in their inboxes.
- Respondents under 35 years are less likely to give out their email address as freely and are more likely to use separate email for situations that may result in possible spam.
- Most define spam as email that is not requested or ends up in the spam folder.
- The sender's name and the subject line are the most common indicators of legitimate email.
- When a suspected spam email is received, most respondents say they delete it without opening it or they move it to the junk folder.
- Nearly half of all respondents say they have never clicked on what they felt was spam. Those who did click on spam say they either made a mistake, are not sure why they did it, sent a note to the company, or were interested in the product or service.
- When suspected spam is received, nearly all say they delete it, either initially or after marking it as spam. A few say they report it to the company, to their ISP or to their email provider.

C. Bots and Bot Mitigation

- While eight out of ten respondents say they are aware of malicious viruses that can control their computer, only two out of ten say it is very likely that their computers will be infected with this type of virus.
- 14% of consumers believe they will never be infected by a bot; 41% think it is not very probable; and 37% describe themselves as neutral.
- Over half of all respondents say that when their computer is infected with a virus it is up to them to fix it. Just under two out of ten respondents say they would use a computer repair professional, while slightly fewer respondents say it is the responsibility of the anti-virus company.
- Overall, 63% of the responses indicated they would allow remote access to remove a virus. Approximately one-fourth said they would repair their computers themselves.
- Consumers who would allow remote access are more likely to "unsubscribe" to unwanted email rather than just delete spam.
- Among those who would allow their infected computers to be repaired remotely, there is an indication that they are more cautious when using email, more aware of bots, and are more likely to say they could be infected with a bot.

D. Virus Infections and Anti-Virus Software Usage

- Approximately half of all respondents believe their anti-virus software updates itself. Over one-fourth say they personally update their own anti-virus software when needed. Just 5% say they either do not use or do not update their anti-virus software.
- One-third of all respondents say their computers have never been infected by a virus. Among those who did experience a virus, one-third relied on themselves, a friend or a family member to repair it; 22% used a repair service; and 11% reported it to their virus company, email hosting company or ISP.
- Additionally, those who have been infected by a virus indicated they are more cautious and realize they are vulnerable when using email, are more aware of viruses, are more likely to repair an infected computer themselves, and are between 24 and 34 years of age.
- Approximately one-third say they are not sure who is most responsible for stopping the creation of computer viruses.

III. Ferris Research, Inc. Observations on Consumer Behavior

Ferris Research Inc. (FRI) specializes in research and analysis for the messaging industry. MAAWG asked the firm's principals David Ferris and Richi Jennings, to review the survey findings and add their insights based on the current state of the email market. Here are their conclusions:

- The more people use email, the more important it becomes for them -- disproportionately so.
- We are astounded -- yet pleasantly surprised -- that so many "non-expert" respondents know about botnets, which is probably due to media coverage. On the other hand, most people do not worry about getting infected themselves.
- We are also pleasantly surprised that 65% of "non-expert" respondents do not respond to spam or see it as a "mistake" to do so.
    - Conversely, a significant number of "non-expert" people -- around 1 in 6 -- do sometimes respond to a spam offer, which is regrettable.
    - It is this level of response that makes spamming a lot more attractive as a business because spam is much more likely to generate revenues at this response rate.
    - Almost every "non-expert," irrespective of age and level of technical savvy, knows how important virus control is. About two thirds of consumers have been hit by a virus, and it is very irritating for them.
    - You might assume that the more technically savvy you are, the less likely you are to be hit by a virus, but that is not true. Our previous research indicates that the more you use computers, the more likely you are to get hit by a virus.

IV. Ferris Research Observations for the Messaging Industry

A. General Industry Recommendations

- Most users do not care about the "this is spam" button. If your company's spam filter learns from users as they mark messages as spam, take steps to encourage correct use of the feature.
- Consider educating your customers to use the feature on false negatives and false positives.
- Consider user interface changes to encourage users to consciously choose between "delete" and "spam."
- Consider reinforcing desired user behavior; make people feel good about helping out and reporting spam. Some suggestions:
    - Offer a monthly drawing or a prize for spam reporters.
    - Offer an award for most spam messages reported each month.
    - For an example of rewarding users by making them feel good, look at the Google functionality where users can report malicious Web pages.
- Consider training the spam filter on messages deleted without being read, with perhaps a lower weighting if users have clicked the Spam button.
    - But do not train on delete-unread if the user has a history of using the Spam button.
    - If the user starts to use the Spam button, stop training on delete-unread.

- Be wary of spammer tactics that spoof the sender, pretending to be people the recipients know:
  - This happens today with fake newsletters and other vehicles.
  - If spammers had access to a wider social graph, we might be in serious trouble. For example, what if...
    - Conficker starts quietly stealing the address books of those infected?
    - Spammers begin leeching data from Facebook, MySpace, and other social media sites?
  - Whitelisting based on the sender is dangerous.
  - This is yet another reason to sign with DKIM and pay attention to received forgeries.

B. *Recommendations for Internet Service Providers and Email Providers*

- Around 10% of users expect their ISPs to fix malware:
  - This contributes to support and churn problems.
  - It represents a differentiation opportunity for ISPs that can show they are better at controlling malware because around a third of users are unhappy with their ISPs' malware control.
- When people get hit with malware, they usually fix it themselves (possibly with a friend), or use a technical support person:
  - They do not expect their ISPs to do the fixing.
  - So ISP remediation is a value-added service or a market differentiator.
- Consider modifying your contractual Terms & Conditions to authorize your company to remotely remediate infected PCs.
  - Do it in such a way as to absolve your organization of responsibility and liability, in case something goes wrong.
  - Also permit subscribers to opt-out from automatic remediation.
- Many users feel the need to install their own spam filters; this is inefficient and inherently less accurate than MX-based spam filters.
  - Consider making user-owned spam filters unnecessary by doing a great job of spam filtering on the server.
  - Consider differentiating yourself by promoting your spam filter accuracy.
  - Consider differentiating yourself by promoting your green credentials, since an accurate spam filter requires less energy use.[3]
  - *Note:* We believe that a significant proportion of the users who said they installed a spam filter were actually using the built-in "filters" in email clients, such as Outlook Express.
- Respondents are unimpressed by the U.S. CAN-SPAM Act (re: responses to questions 8 and 15)
  - If you are involved in successful civil prosecutions of spammers, consider publicizing to your users how you are reinvesting spammer fines to protect Internet users from spam.
  - Users would support stronger governmental action against malware. Is this a lobbying opportunity?

[3] Report: “The Carbon Footprint of Spam”, by ICF International and Richi Jennings 2009
http://richi.co.uk/blog/2009/04/spam-and-its-carbon-footprint.html

C. Recommendations for Anti-Virus and Anti-Malware Vendors

- Tune your filters to avoid false positives for the most "important" types of email content identified in the survey, which are from friends/family; receipts and shipping notifications; and from banking and other financial information.
- Users make heavy use of email for banking and billing statements, especially people aged 25 to 44, which should be a driver or target for anti-phishing technology.
- A surprisingly large proportion of people -- around 1 in 6 -- are prepared to make an effort to report spam. These efforts can be harvested by vendors to improve their filters

NOTE: Section V. Detailed Findings with responses to the questions and charts can be found be Part 2 of this report, which is a separate PDF file.

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.

© 2009 Messaging Anti-Abuse Working Group (MAAWG)