Ipsos Public Affairs
The Social Research and Corporate Reputation Specialists

Key Findings of the 2010 MAAWG Email Security Awareness and Usage Survey

(Issued March 2010)

Survey Background

This is the second year the Messaging Anti-Abuse Working Group has surveyed consumers' awareness of email security practices. While the 2009 survey looked at North American consumers, this survey expanded the effort to both North America and Western Europe. This document summarizes the key findings. The complete survey report with all the data is available on the MAAWG Web site at www.MAAWG.org.

Those surveyed were general consumers who indicated they did not have an IT professional managing their email address and were therefore generally responsible for their email experience. Since we were interested in consumers' habits, we did not differentiate between ISPs and ESPs, but used these terms to refer to the service where consumers obtain their email.

Results Overview

Half of email users in North America and in Western Europe have opened or accessed spam, and large proportions – representing tens of millions of consumers – have taken action like clicking on links or opening attachments that could leave them susceptible to their computers being infected.

Furthermore, nearly half of those who have accessed spam (46%) have done so intentionally – to unsubscribe, out of curiosity, or out of interest in the products or services being offered.

In addition, many users do not typically flag or report spam or fraudulent email. Younger users both generally consider themselves more experienced in terms of email security but also are more likely to engage in risky behavior, such as opening or clicking on spam.

Across the six countries surveyed, 84% were aware of the concept of bots. Yet, most think that they are immune from these viruses, with only a third saying they consider it likely that they could get a bot on their computer. While most would rely on their anti-virus software to alert them, one in five are unsure as to how they would recognize a bot infection on their computer.

Among various types of organizations, Internet/email service providers and anti-virus software companies are those most widely perceived as responsible for stopping the spread of viruses, fraudulent email and spam. Less than half of users think that stopping the spread of viruses and spam is their own responsibility, but they tend to rate themselves better at doing it than all organizations, except for anti-virus software companies which get the highest marks.

Context: Experience, Email Preferences and Security Habits

On average, across the six target countries, nearly half of email users surveyed (44%) classify themselves as "somewhat experienced" when it comes to security on the Internet, including firewalls, spam, junk mail and computer viruses. Other users are more likely to consider themselves as "not very" or "not at all experienced" (36%) rather than consider themselves "an expert" or "very experienced" (20%).

- In Germany 33% of users describe themselves as "an expert" or "very experienced" (33%), followed by those in the U.K. (22%), the U.S. (21%) and Spain (19%). Just 8% of French email users describe themselves as such.

- There are also significant differences across age groups, with younger users being much more likely to describe themselves as being experienced with Internet security than are older users.

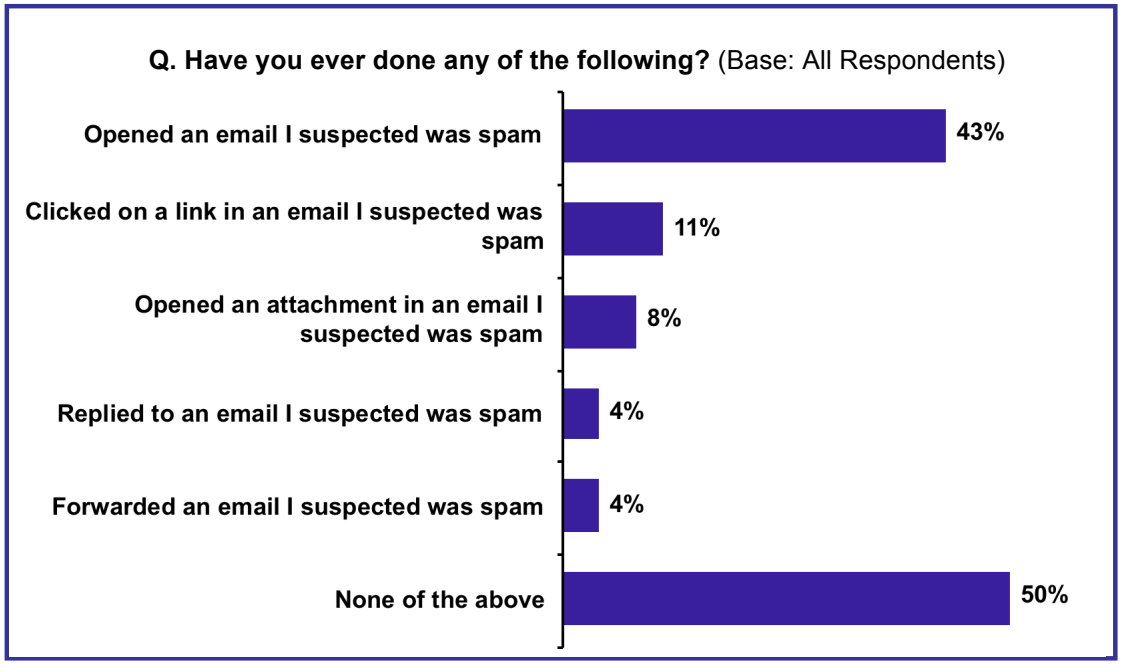
In every country, at least three-quarters of respondents consider email from friends and family to be extremely or very important (82% extremely/very important on average across the six countries). Email users also tend to place a great deal of importance on receipts or shipping details for purchases (70%), notifications of bills to be paid (64%), and notifications from a bank or another financial institution (58%). Email users in all countries tend to give less importance to newsletters (20%), marketing materials (15%) and other emails that they have subscribed to (22%).

- Email users in France and Germany tend to place less importance on notifications from their financial institutions than do their counterparts in other countries surveyed.

At least nine in ten respondents in each country say their anti-virus software is updated regularly. Most commonly, respondents say that it does so automatically (46%), that they do it themselves (33%), or that someone else takes care of it (15%). Very few (2%) say that no one updates their anti-virus software.

Who Is Opening Spam – and Why?

Four in ten (43%) say that they have opened an email that they suspected was spam, though fewer have taken more risky behaviors such as clicking on a link (11%), opening an attachment (8%), replying to (4%) or forwarding (4%) an email they suspected was spam. These riskier behaviors are more common among men and email users under 35 – the same demographic groups who are more likely to consider themselves experienced when it comes to Internet security threats. Younger users are more likely not only to open spam (50% under 35 vs. 40% of those aged 35-54 and 36% of those aged 55 and older), but also to click on a link in an email they suspected was spam (13% vs. 10% and 9%, respectively) and to reply to these emails (5% vs. 4% and 2%, respectively).



Among those who have opened a suspicious email, over half (57%) say they have done so because they weren't sure it was spam and one third (33%) say they have done so by accident. However, nearly half (46%) report having accessed spam intentionally – to unsubscribe or complain to the sender

(25%), to see what would happen (18%), and/or to learn more about the products or services being offered (15%). With so many users clicking on links (11%) or replying to spam (4%), this amounts to millions of consumers engaging with spam.

- In the 2009 study, the 58% of online respondents who opened or clicked on spam were most likely to say they "made a mistake," "sent a note," or said that they were "interested in the product/service."

Typically, three in five users (61%) say that when they suspect an email is spam, they usually do not open it. About four in ten move it to their junk mail folder (44%) or hit the "spam" button (39%). Fewer report it to their ISP or ESP (9%) or to a third party spam reporting service or government agency (7%), though U.S. users are more likely to do so than are their counterparts in other countries. However, nearly half delete it without flagging it as being spam (47%).

When they receive emails that they worry may be fraudulent, users tend to react as they do with spam: By not opening the message (60%), deleting it without flagging it as being spam (41%), moving it to their junk mail folder (34%) or hitting the "spam" button (32%). Users are slightly more likely to report fraudulent email than they are to report spam to their ISP or ESP or to a third-party spam reporting service or government agency. One in five say that they typically report it to the legitimate company or institution. Also, one in six say that they usually run their anti-virus software when they receive an email they think may be fraudulent.

- The findings among American respondents are consistent with those of the 2009 study, despite a change in wording.

Email users tend to look for a variety of signs in order to identify spam in their inbox, particularly the sender's name or address (73%) and the subject line (67%). These are the top spam indicators in all six countries. Roughly half also say that unusual language, the content of the email, the receiver's name or address and spelling mistakes or poor grammar are signs that an email may be spam.

- Respondents in Spain and France tend to rely less on each of these indicators when deciding what is spam and what is legitimate email.

Awareness, Concern about Bots Lagging

Three in five users (58%) on average say that their computer has been affected by a virus. Experience with a virus is most common in Spain (69%) and Canada (68%), but least common in Germany (45%).

- In 2009, one third reported that they had "never been infected" with a virus.

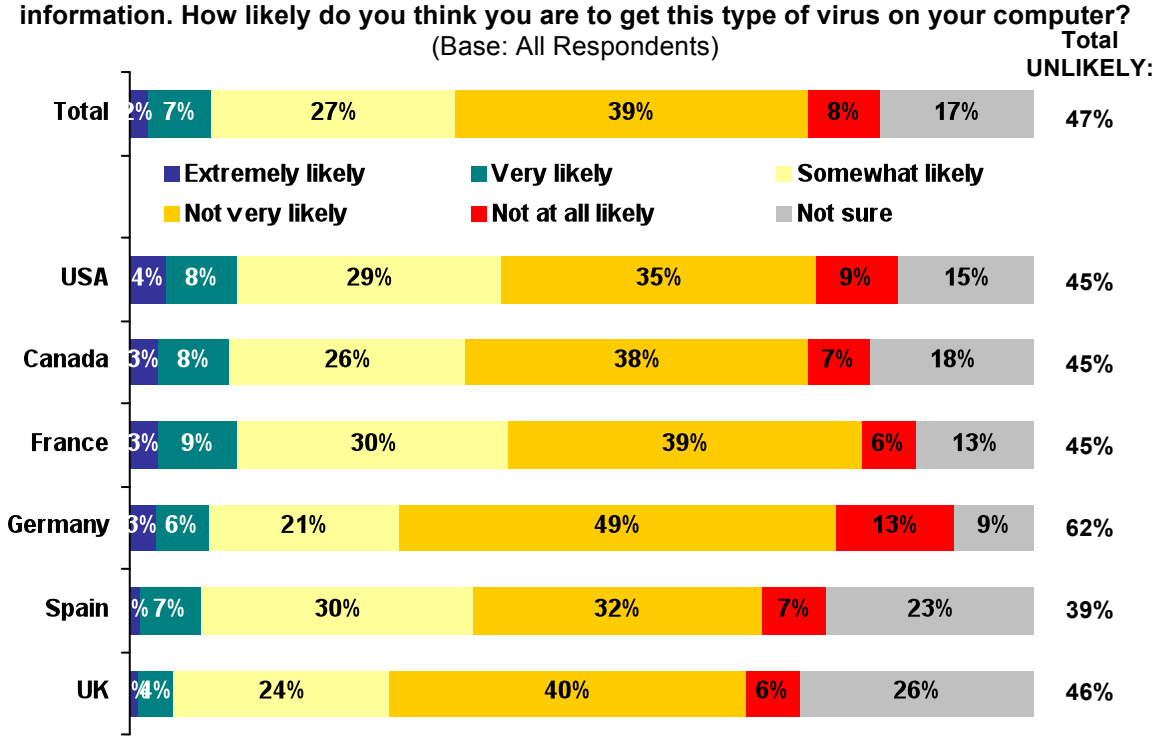
Despite the prevalence of viruses, less than half (47%) have heard of the term "bot" or "botnet," though 84% are aware of the concept of bots, i.e., "malicious viruses that can control their computer without their knowledge and may then use their computer to spread spam or steal their personal information." Awareness of the term "bot" or "botnet" is highest in English-speaking countries and Germany, while lower in Spain and France.

- These figures are very consistent with the findings from last year's study, when 77% of U.S. online respondents said that they were aware of these types of viruses.

Though a majority of users say that their computer has been infected by a virus, only 36% say that they are at least somewhat likely to get a bot on their computer. French users are more likely to be concerned about getting a bot than others, especially when compared to British and German users.

- Across the six countries, 47% say they are not very or not at all likely to get a bot. In the U.S., 45% say so, mirroring the results of the 2009 study (43%).

Q. A 'bot' or 'botnet' is a malicious virus that can control your computer without your knowledge and may then use your computer to spread spam or steal your personal information. How likely do you think you are to get this type of virus on your computer?
(Base: All Respondents)



Asked how they would find out if their computer were to get a bot, users are most likely to say they would be alerted by their anti-virus software (66%). At least half also say they would know if their computer was not functioning properly or was running very slowly or if they noticed a program they had not installed (52%, respectively).

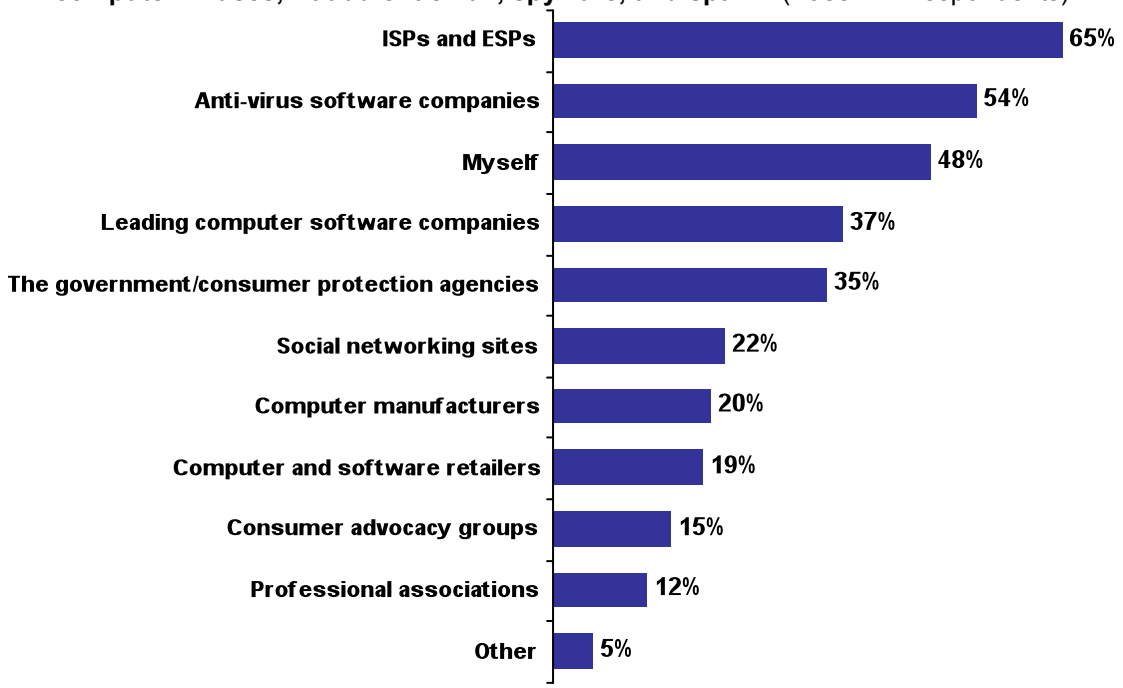
Over half of users in Canada and France, and about four in ten elsewhere, say they would recognize they had a bot if their friends told them they were receiving spam from their email address. A majority of Germans would look out for unusual error messages.

At the same time, one in five say they are not sure how they would know if their computer had a bot. Spanish users are those most likely to be unsure how to recognize a bot (28%).

Whose Responsibility Is It to Stop Bots?

When it comes to stopping the spread of viruses, fraudulent email, spyware and spam, email users are most likely to hold ISPs and ESPs (65%) and anti-virus software companies (54%) responsible. Less than half of users (48%) hold themselves personally responsible for stopping these threats, though this proportion is even lower in France (30%) and Spain (37%).

Q. Who do you feel should be most responsible for stopping the spreading of computer viruses, fraudulent email, spyware, and spam? (Base: All Respondents)



Across countries, respondents tend to rate anti-virus software companies (67% very/fairly good) and themselves (56%) as performing best when it comes to stopping the spread of viruses, fraudulent email, spyware and spam. In contrast, they tend to be most critical of government or consumer advocacy agencies (34% very/fairly poor) and social networking sites (34%).

- Anti-virus software companies were also top-rated in the 2009 study.

If their computer were to get a virus, spyware or bot, users are most likely to say that they would hold themselves responsible for fixing it (58%). Many also report that they would turn to their anti-virus software company to have their computer repaired (43%).

Methodology

Interviewing was conducted online among Ipsos panel members aged 18 and older in the U.S., Canada, the U.K., France, Spain and Germany between January 8 and 21, 2010. All respondents reported having at least one email address for which they manage the security (and do not rely on an IT person or service).

Country	Sample Size
U.S.	1,082
Canada	548
France	512
Germany	522
Spain	527
U.K.	525
TOTAL	*3,716*

Quotas and weighting were employed to ensure that the achieved sample is representative of the online population in each country in terms of gender, age and education level, based on official statistics from local census organizations, including the U.S. Census Bureau and Eurostat.

Multi-country data were aggregated so that each country was given equal weight, regardless of the achieved sample size.

The complete survey report with more charts, data and the questionnaires in multiple languages is available at the MAAWG Web site, www.MAAWG.org.