2010 MAAWG Email Security Awareness and Usage Report

Issued March 2010

Ipsos Public Affairs
1700 Broadway, 15th Floor
New York NY 10019
Tel: 212.265.3200
Fax: 212.265.3790
www.ipsos.com

TABLE OF CONTENTS

1. Background and Objectives

Messaging abuse now spans technologies and platforms, affecting online and wireless communications, and permeating geographic boundaries. The Messaging Anti-Abuse Working Group (MAAWG), in response, has adopted a holistic perspective on the issue: promoting and publicizing technology solutions, encouraging industry collaboration for codes of behavior, and guiding and supporting public policy for safeguarding messages.

MAAWG strives to inform its efforts and to provide a fresh and needed outlook on the prevalence and impact of message abuse globally by continuously gaining insight into the perceptions, attitudes and behavior of technology consumers and general email users with regards to the risks they incur.

In order to further a first survey of general email users in the United States conducted and released in early 2009, MAAWG undertook to conduct a new survey in January 2010 with a scope that extends beyond the U.S. to Canada and four Western European countries – France, Germany, Spain and the United Kingdom.

MAAWG is proud to present in this document the results of its 2010 survey on attitudes and behaviors of email users towards message abuse safety and computer viruses.

We believe that the research successfully met the following objectives:

- Measuring the levels of email users' awareness of spam issues;
- Understanding how email users distinguish legitimate email from spam;
- Measuring the level of awareness of messaging threats and perceived vulnerability;
- Tracking changes in response patterns among U.S. respondents;
- Providing a benchmark for future research; and
- Providing research results as basis for outreach and communication campaigns.

2. Methodology

Target Audience

The universe of the survey consists of adults aged 18 and older who have at least one email address for which they handle the security (i.e., do not rely on an IT person/service for that email address).

Interviewing Method and Sample Source

The survey was conducted with an online interviewing methodology in each one of the six countries. This approach was deemed to be particularly appropriate considering the topic and the definition of the population.

All interviewing was conducted January 8-21, 2010. Survey participants are all members of Ipsos' opt-in consumer panels in each of the six markets and were invited to participate via email. They were asked a series of screening questions to ensure that they were qualified to participate.

Sample Size, Quotas and Weighting

A total of 3,716 respondents were interviewed across the six countries. The final achieved sample is distributed as follows:

	Sample Size
USA	1,082
Canada	548
France	512
Germany	522
Spain	527
UK	525
North America Total	1,630
Western Europe Total	2,086
TOTAL	**3,716**

Target quotas and sample balancing weights were employed to ensure that the achieved samples are representative of the online population of each country in terms of gender, age and education level, based on official statistics from the U.S Census Bureau, Statistics Canada, Eurostat and Spain's Instituto Nacional de Estadística. Multi-country data (i.e., results reported as the "total" or "average" of data from multiple countries) were aggregated so that each country is given equal weight, regardless of the achieved sample size in each country.

Margins of error

The estimated margin of error with a 95% level of confidence of a survey with an *unweighted probability sample* of the same size and a 100% response rate would be of +/-3 percentage points around the U.S. data (N=1,082) and of +/-4 points around the data from each one of the other five countries (N=512-548) of what the results would have been had the entire population of email users in that country been polled. All sample surveys and polls may be subject to other sources of error, including, but not limited to coverage error, and measurement error.

Questionnaire

The same questions were asked in all countries. To avoid order bias, the order of answer items at many questions was randomized.

The survey instrument was designed in English. All translations were checked for accuracy against the original English version and for clarity. Every language version of the questionnaire is provided in the Appendix.

Interviews lasted approximately 12 minutes on average.

Comparisons with the 2009 Survey

The following caveats should be applied when comparing the results of the U.S. data from the 2010 survey conducted by Ipsos with those of the 2009 study, which was conducted by Insight Worldwide Research:

- In the 2009 survey, self-reported email and security "experts" were excluded. However, in the 2010 research, "experts" were allowed to participate in the survey (and only make up 5% of the sample).
- The 2009 survey used a combined online and telephone methodology (400 interviews with each method). The 2010 survey was conducted entirely online.
- While many questions are similar, the wording or the list of answer options to many of them was altered between 2009 and 2010. This was generally done to refine the survey based on our experience and improve the question clarity.

For these reasons, all data comparisons between the 2009 and 2010 surveys made in the report are only directional in nature.

3. Key Findings

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 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, 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

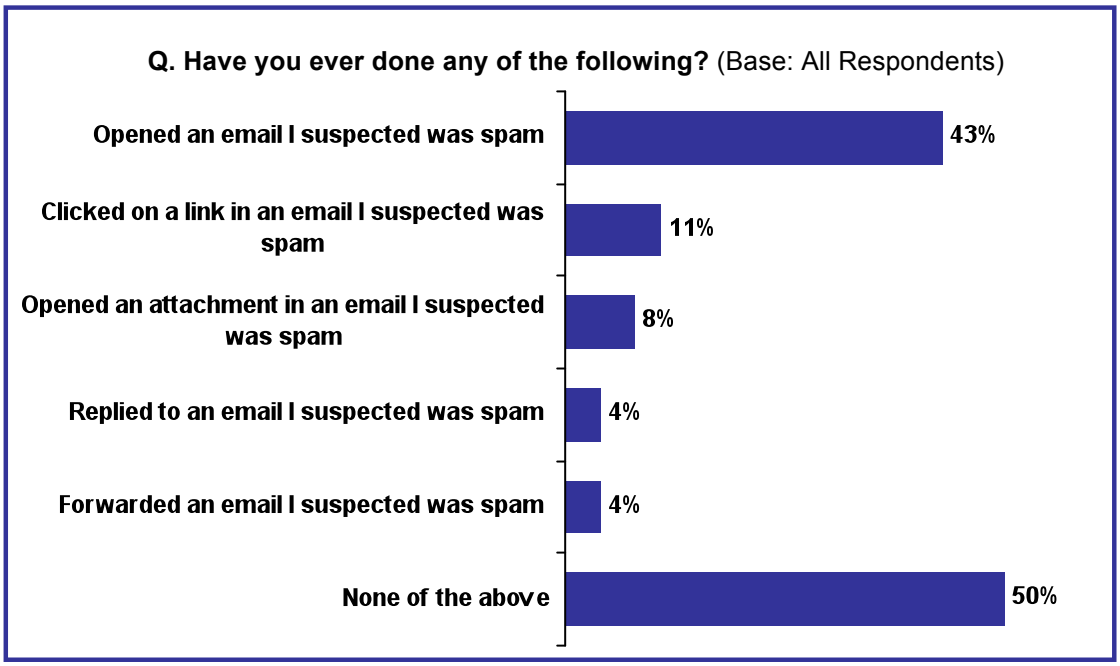
countries). Email users also tend to place a great deal of importance on receipts or shipping details for purchases (70%), notifications of bills to be paid (64%), and notifications from a bank or another financial institution (58%). Email users in all countries tend to give less importance to newsletters (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.

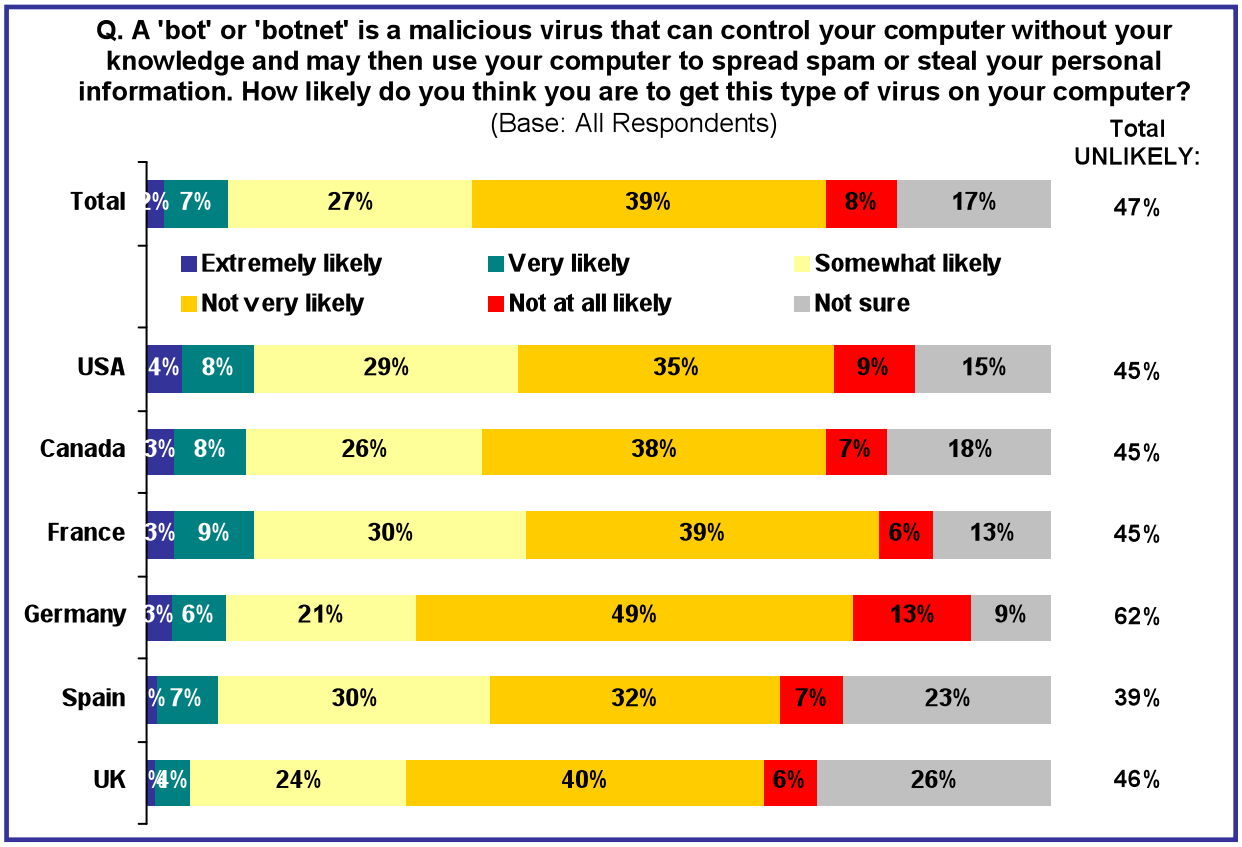
Awareness, Concern about Bots Lagging

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%).



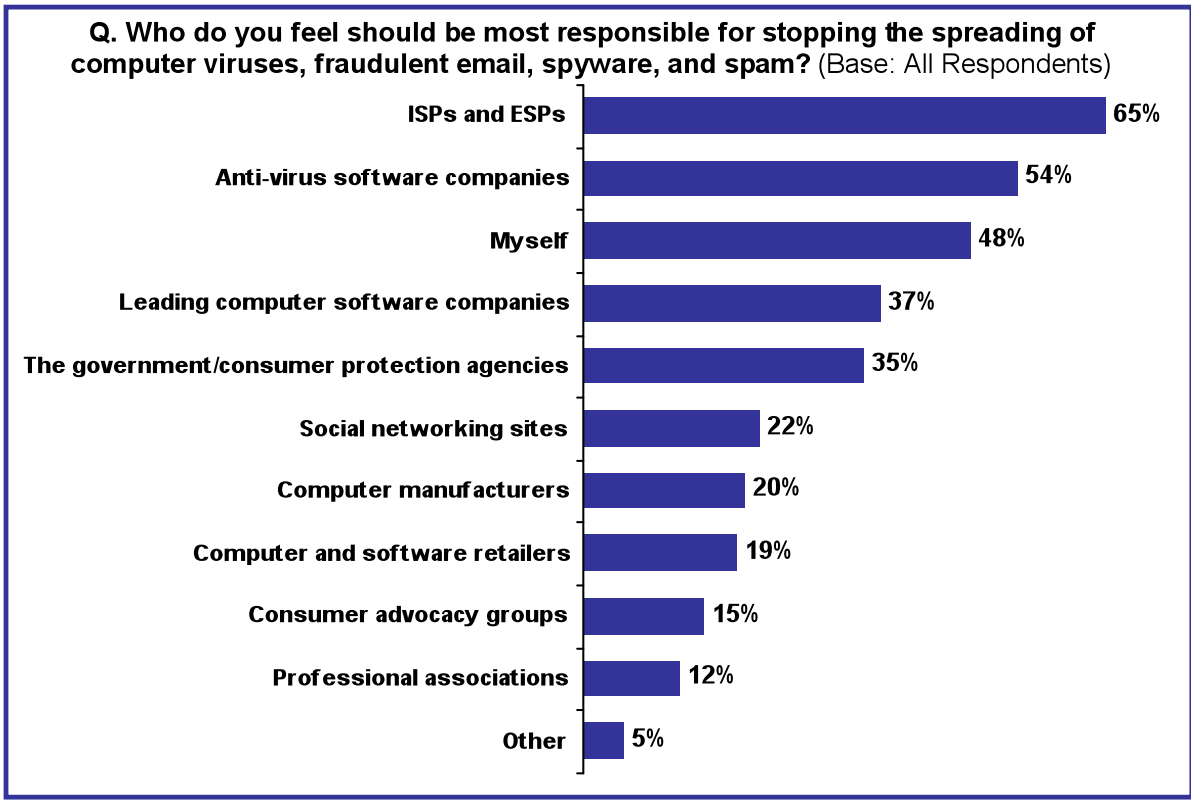
Asked how they would find out if their computer were to get a bot, users are most likely to say they would be alerted by their anti-virus software (66%). At least half also say they would know if their computer was not functioning properly or was running very slowly or if they noticed a program they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



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%).

4. Detailed Findings: Experience, Security Habits and Email Preferences

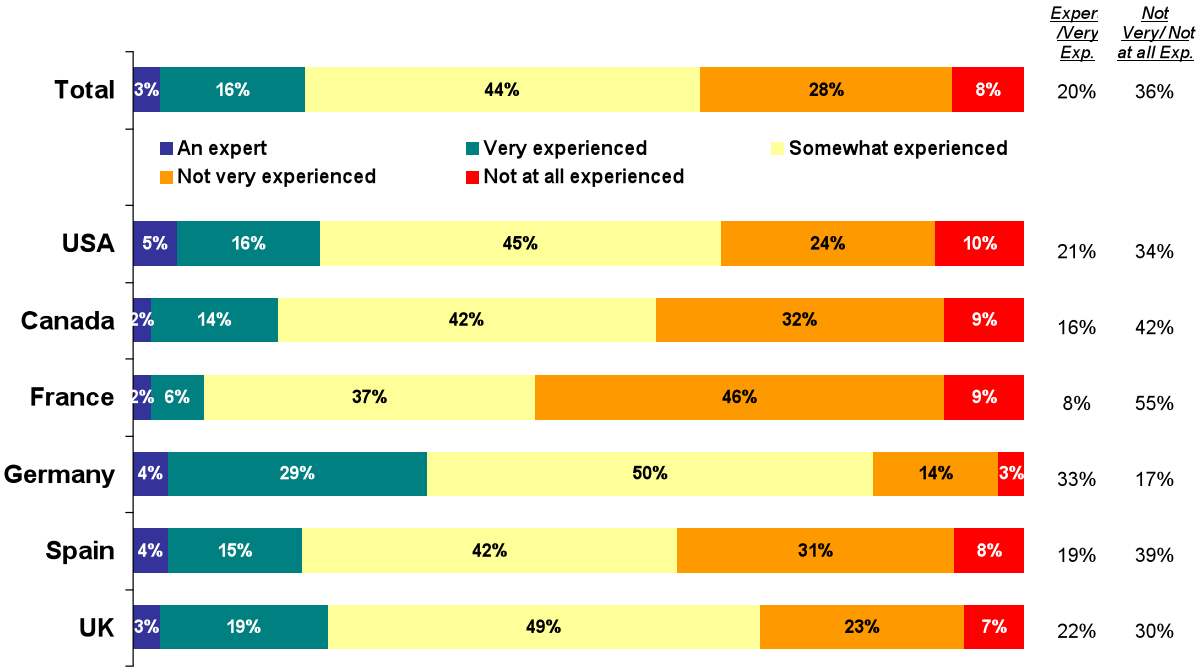
Experience with Internet Security Threats

On average, across the six target markets, nearly half of email users surveyed (44%) describe themselves as "somewhat experienced" when it comes to security on the Internet, including firewalls, spam, junk mail and computer viruses. They represent the largest contingent of email users in every country except France.

Other users are more likely to portray themselves as "not very" or "not at all experienced" (36%) than as "an expert" or "very experienced" (20%)

- Differences across countries are significant. The proportion of email users who describe themselves as very experienced or experts ranges from as much as 33% in Germany to only 8% in France where a majority (55%) report having little or no experience regarding Internet security.

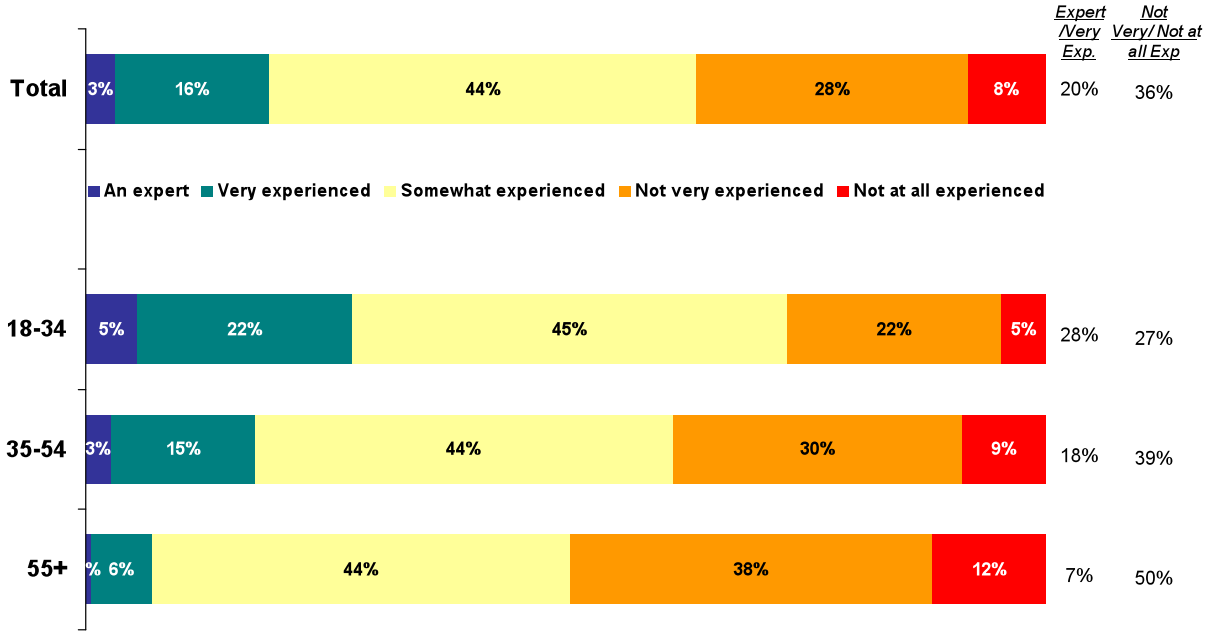
Q1. How would you describe yourself when it comes to your experience with security on the Internet, including firewalls, spam, junk mail and computer viruses? (Base: All Respondents)



- Men are twice as likely as women to identify themselves as being experts or very experienced (27% vs. 13%).
- Experience with Internet security issues decreases with age. While 28% of email users aged 18 to 34 describe themselves as being experts or very experienced, 18% of those aged 35 to 54 and only 7% of those aged 55 and older concur.

- Users who are also most likely to describe themselves as experts or very experienced include those who have a higher level of education (26%) and those who are employed (22%).
- Differences when it comes to perceived experience may explain some of the variations observed across markets when it comes to other Internet security-related attitudes and behavior.

Q1. How would you describe yourself when it comes to your experience with security on the Internet, including firewalls, spam, junk mail and computer viruses? (Base: All Respondents)



In the 2009 U.S. study, self-described "experts" were not included in the survey. Without those email users, 64% of respondents interviewed by telephone or online reported that they were "very" or "somewhat experienced" with Internet security while 36% said that they were "not very" or "not at all experienced". In the 2010 all-online study, experts were allowed in and make up 5% of all respondents, 61% describe themselves as very or somewhat experienced and 34% as not very or not at all experienced.

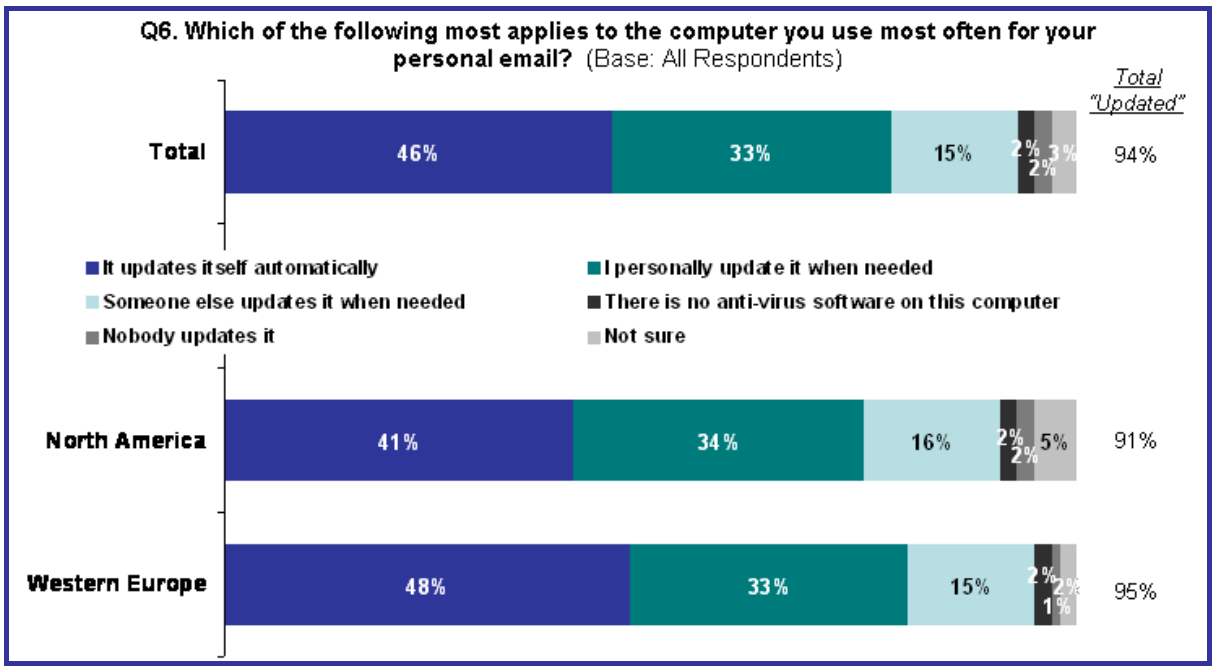
Keeping Anti-virus Software Updated

Although many feel they have limited experience with Internet security, more than nine in ten (94%) report that they keep their anti-virus software updated. Most commonly, the software is said to update itself automatically (46%), though a third say that they personally update it and 15% say that someone else takes care of this task for them. Only 2% say their anti-virus software is not updated and 3% say they are unsure.

In 2009, nine in ten U.S. users surveyed also said that their anti-virus software was updated, most commonly automatically (51%).

- Automatic updating is reportedly more common in Germany (60%) and France (50%) than it is in other markets, especially the U.S. (36%).
- North American users are somewhat more likely than their European counterparts to say they are not sure whether their anti-virus software is updated (5% vs. 2%).
- Women are more likely than men to say that someone updates their software for them (21% vs. 10%).
- Users under the age of 35 are less likely than older adults to report having anti-virus updated (92% vs. 95%).

Those whose anti-virus software is not updated mostly say this is because they are unsure about how to update it (30%), because they don't have the time (24%), or due to the expense (14%). In addition, 12% say that they never get a virus and 9% say that their software doesn't need to be updated. An additional 12% say that none of these reasons explain why their software is not updated.



Importance Placed on Different Types of Email

Among various types of email, personal email from friends and family members is most widely considered to be extremely or very important and is rated as such by 82% of users surveyed, including no fewer than three quarters in any country.

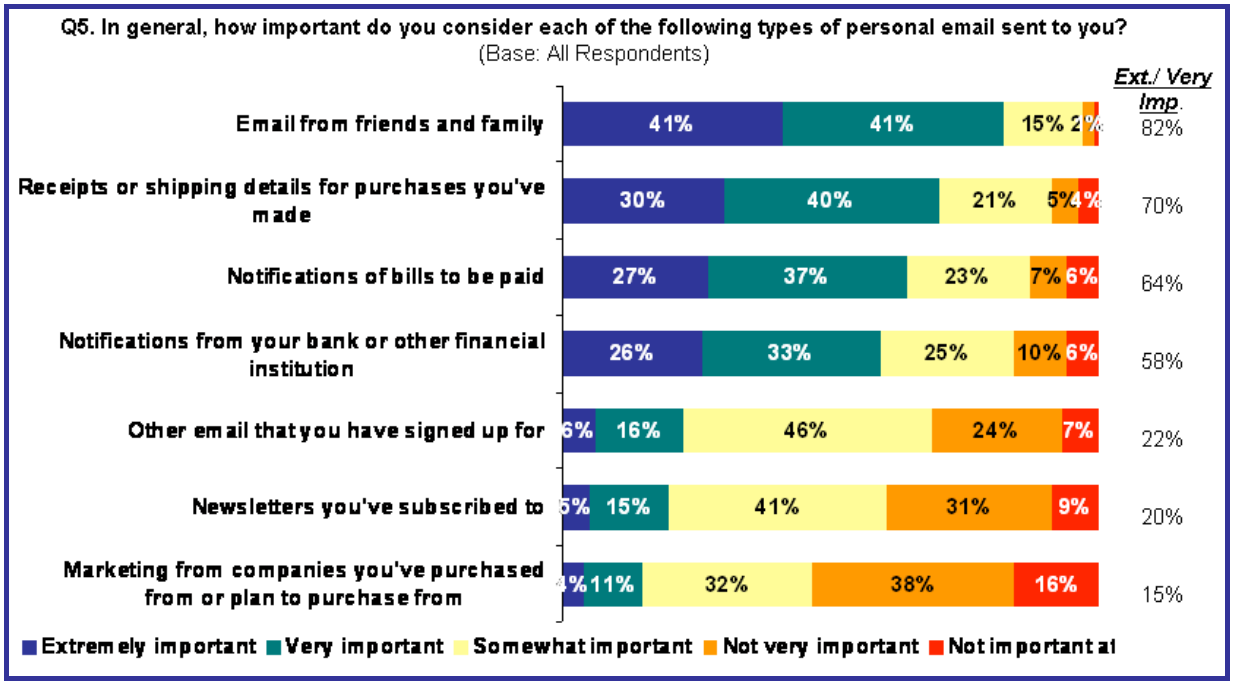
Overall, majorities also place a great deal of importance on several types of financial email, including those with receipts or shipping details for purchases (70% say they are extremely or very important), bill notifications (64%), and bank notifications (58%).

Email users tend to attach far less importance to newsletters (20%), marketing from companies they have made purchases from (15%), and "other email that they have signed up for" (22%).

This hierarchy of email types mirrors the findings from the 2009 study.

Among geographic and demographic differences:

- Users in France and Germany are less likely than those in other countries to rate these finance-related emails as important.
- Women tend to be more likely than men to view both personal and financial types of email as important.
- Users under 35 are more likely than those who are older to say that billing notifications and marketing materials are important to them, while adults aged 55 and older are more likely than those who are younger to think of newsletters as being important.



5. Detailed Findings: What Is Seen as Spam, Who Is Opening It – and Why?

Defining Spam

Users tend to define "spam" in a variety of ways. The types of email they are most likely to label as "spam" are, in order: email they "did not request" (69%), "email from porn, pills, casinos, etc." (59%), and "email that contains a virus or phishing scheme" (59%).

Similarly, in the 2009 survey, spam was most commonly defined by online respondents as "email that is not requested" (69%), "email from porn, pills, casinos, etc." (63%), and "phishing email" (62%).

Roughly half also consider email that violates anti-spamming regulations (52%), email in their spam or junk mail folder (51%), and email from sources that they cannot 'unsubscribe' from (48%) to be spam.

However, few would classify email that they once requested but no longer want (16%) or jokes and silly messages that are forwarded to them (15%) as spam.

Users in France and, in particular, Spain, tend to have a more limited definition of what constitutes spam, as they tend to be less likely to classify each of these types of email as spam. In contrast, users in the U.S. and U.K. tend to be most willing to label various categories of email as spam.

Users aged 55 and older also tend to be quicker to characterize email as spam than are users aged 18 to 54, particularly when it comes to email that violates anti-spamming regulations (61% vs. 50%), email in their spam or junk mail folder (57% vs. 50%), email that they once requested but no longer want (22% vs. 15%), and jokes and silly messages that are forwarded to them (20% vs. 14%).

Email users with a higher level of education also prove less tolerant of spam, as they are more likely than those who have the equivalent of a high school education or less to categorize many types of email as being spam, including: email from porn, pills, body part enlargement, online casinos, etc. (65% vs. 53%); email that contains a virus or phishing scheme (61% vs. 53%); email that violates anti-spamming regulations (55% vs. 46%); and email from sources that they cannot "unsubscribe" from (51% vs. 43%).

- Interestingly, those who have opened spam in the past are more likely to brand the various types of email as spam than are those who have not opened spam messages. Perhaps their past experiences with spam have made them more wary of these types of messages.

Q8. How do you personally define spam? (Base: All Respondents)

	Total	USA	Canada	France	Germany	Spain	UK
Email I did not request	**69%**	72%	72%	62%	68%	67%	73%
Email from porn, pills, body part enlargement, online casinos, etc.	**59%**	71%	65%	42%	66%	41%	72%
Email that contains a virus or 'phishing' scheme	**59%**	70%	63%	52%	65%	36%	67%
Email that violates anti-spamming regulations	**52%**	63%	55%	36%	59%	35%	61%
Email in my spam or junk mail folder	**51%**	59%	55%	44%	50%	44%	55%
Email from sources that I cannot 'unsubscribe' from	**48%**	63%	55%	34%	51%	28%	60%
Email that I once requested, but no longer want	**16%**	22%	17%	13%	12%	15%	21%
Jokes and silly messages forwarded to me	**15%**	18%	19%	15%	13%	10%	16%
Other	**4%**	5%	4%	2%	5%	8%	3%

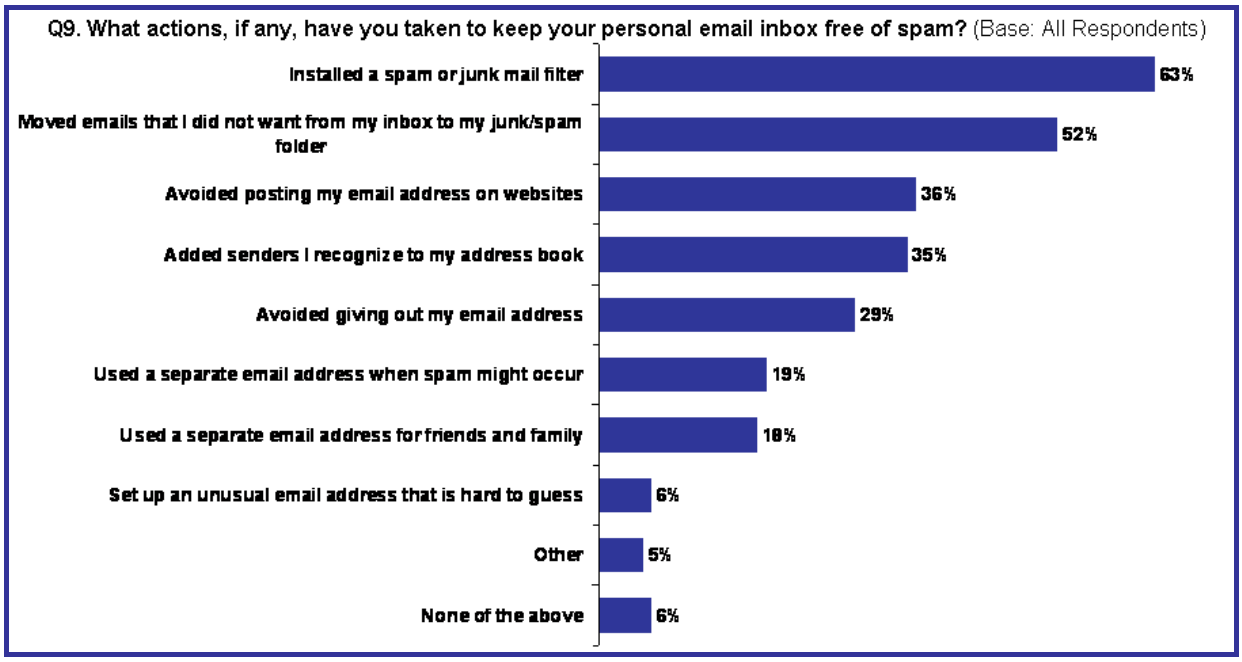
Preventing and Identifying Spam

In order to manage their inbox and keep it free of spam, majorities of email users say that they have installed a spam filter (63%) or moved emails that they did not want from their inbox to their junk/spam folder (52%).

Similarly, 64% of online respondents in last year's study reported that they had installed a spam filter in order to avoid receiving spam or junk email in their personal email.

Roughly a third say that they have avoided posting their email address on Web sites (36%), added senders they recognize to their address book (35%), or avoided giving out their email address (29%). Fewer use separate email addresses either when spam might occur (19%) or for friends and family (18%), and just 6% have created an unusual email address as a means of keeping their personal inbox free of spam. However, more than one in twenty (6%) have not taken any of these measures in an effort to prevent spam.

Though the question was worded a bit differently in the 2009 study, the results showed that 14% of online respondents were not taking any action to prevent spam in their inboxes.



- The prevalence of spam filter usage as a means of keeping one's inbox spam-free varies across markets. Among the six countries surveyed, it is highest in Germany (72%) and France (69%) and lowest in Spain (50%). German users are also more likely to move spam from their inbox to a junk folder (64%) than their counterparts in other countries, especially France (38%).
- Canadian users are those most likely to avoid posting their email address online (46%). Those in the U.S., Canada and Germany are most likely to set up separate email addresses in order to avoid receiving spam.
- Email users aged 35 and older are much more likely to say that they have installed a spam filter than are those who are younger (67% vs. 57%), though younger users are more likely to have set up a separate email address when spam might occur (24% vs. 16%) or for friends and family (22% vs. 16%). Men are also more likely than are women to create alternate email accounts to avoid spam.

As seen in the earlier U.S. study, across the six markets users look to a variety of indicators in order to identify spam, most commonly the sender's name or address (73%) and the subject line (67%). Majorities also think of unusual language (53%) and the content of an email (53%) as tip-offs that an email may be spam. At least four in ten also look at the receiver's name or address (46%) and spelling mistakes or poor grammar (43%) in order to decide what is spam and what is legitimate email, while 30% look for icons or other visual indicators in their inbox.

Few differentiate spam based on the time of day or night when an email was sent (9%) and fewer yet (6%) use some other type of indicator while 2% rely on none of these. Less than 1% of email users say they want all of the email that they receive.

Q10. When going through your email box and deciding what email is spam and what is legitimate, what indicators do you rely on to help you decide? (Base: All Respondents)

	Total	USA	Canada	France	Germany	Spain	UK
The sender's name or address	**73%**	75%	77%	71%	76%	70%	72%
The subject line	**67%**	74%	70%	52%	71%	54%	79%
Unusual language	**53%**	59%	54%	52%	56%	36%	60%
The content of the email	**53%**	59%	57%	43%	50%	43%	65%
The receiver's name or address	**46%**	49%	50%	42%	46%	41%	49%
Spelling mistakes/poor grammar	**43%**	53%	45%	44%	35%	23%	57%
The icons/visual indicators that appear in inbox beside the msg	**30%**	31%	32%	25%	33%	23%	34%
The time of day/night when sent	**9%**	14%	11%	7%	4%	5%	13%
Other	**6%**	9%	7%	4%	5%	5%	5%
I want all the email I receive	**1%**	0%	1%	1%	1%	1%	0%
None of the above	**2%**	2%	3%	2%	2%	2%	2%

- Users in France and Spain are least likely to look at each of these as indicators that an email is spam while those in the U.S. and U.K. are most likely to do so.
- Women are more likely than men to look at the sender's name or address (76% vs. 71%) and icons (32% vs. 28%) while men are more likely to make their decision based on the email's contents (56% vs. 49%) or the spelling and grammar (45% vs. 40%).
- Those who consider themselves an expert or very experienced when it comes to Internet security are more likely than those with little experience to use each of these indicators, particularly the subject line (76% vs. 56%), the content (63% vs. 45%) and spelling/grammar (52% vs. 36%).

Email users aged 55 and older are also more likely than those under the age of 35 to use many of these indicators.

Managing Their Inbox

While six in ten email users (61%) say that they usually refrain from opening emails that they suspect may be spam, only 39% mention taking the extra step of flagging it as spam and 44% say they move it to a junk folder. Very few go even further by reporting it to their Internet or email service provider (9%) or taking advantage of third-party spam or email abuse reporting services or a government agency (7%). Rather, nearly half (47%) say that they typically delete these messages without marking them as spam.

Nearly a quarter (24%) say that they typically use the unsubscribe link in the email and 16% say that they tend to read the messages but avoid clicking on any links or attachments.

Just 1% say receiving spam prompts them to change their email address. The same proportion (1%) report that they do not usually take any of these steps when they receive an email they suspect is spam.

The 2009 data showed that nearly three quarters of U.S. users (73%) typically "deleted spam without opening it" while 55% "moved it to a junk folder." Similar proportions of

online respondents in 2009 said that they reported spam to their email provider (14%) or their ISP (8%). Similar observations can be made in 2010 although the question language varies somewhat. U.S. respondents in the 2010 study are a bit more likely to use the unsubscribe link than was seen in the 2009 study (27% vs. 18%).

Q11. When you receive email that you think is spam, what do you usually do?
(Base: All Respondents)

	Total	USA	Canada	France	Germany	Spain	UK
Do not open it	**61%**	64%	65%	62%	64%	50%	61%
Delete it without marking it as spam or junk	**47%**	46%	52%	52%	40%	43%	45%
Move to a 'junk mail' folder	**44%**	45%	47%	43%	46%	39%	48%
Hit the 'This Is Spam' button	**39%**	49%	35%	26%	45%	35%	43%
Use the 'Unsubscribe' link	**24%**	27%	25%	27%	20%	15%	27%
Read it without opening any attachment/clicking on link	**16%**	16%	14%	15%	16%	14%	19%
Report it to my ISP or ESP	**9%**	16%	9%	5%	8%	3%	11%
Report to a 3rd party spam/email-abuse reporting service/gov't agency	**7%**	13%	5%	5%	7%	3%	8%
Change my email address	**1%**	2%	2%	1%	1%	1%	0%
Other	**3%**	3%	2%	2%	3%	4%	2%
None of the above	**1%**	2%	1%	1%	1%	1%	1%

- Canadian and French users are most likely to just delete spam without flagging it or reporting it (52%, respectively).
- Those in the U.S. tend to take a more active role in managing spam, as they are most likely to use the "this is spam" button (49%) as well as to report spam either to their ISP or ESP (16%) or to a reporting service or government agency (13%).
- Significant differences also emerge across age groups when it comes to handling spam. Users under 35 are more likely than those 55 and older to put their spam button to use (41% vs. 34%) while these older adults are more likely to just delete suspected spam messages without flagging it as such first (54% vs. 44%). However, they are also more likely than are those under 35 to say that they do not open spam at all (68% vs. 55%).
- Those who consider themselves at least "very experienced" with Internet security issues are more likely that those who have little to no experience to actively manage spam, by moving spam to a junk folder (52% vs. 37%), hitting the spam button (55% vs. 25%) and reporting these messages to their ISPs or ESPs (13% vs. 6%) or to a reporting service (12% vs. 3%).

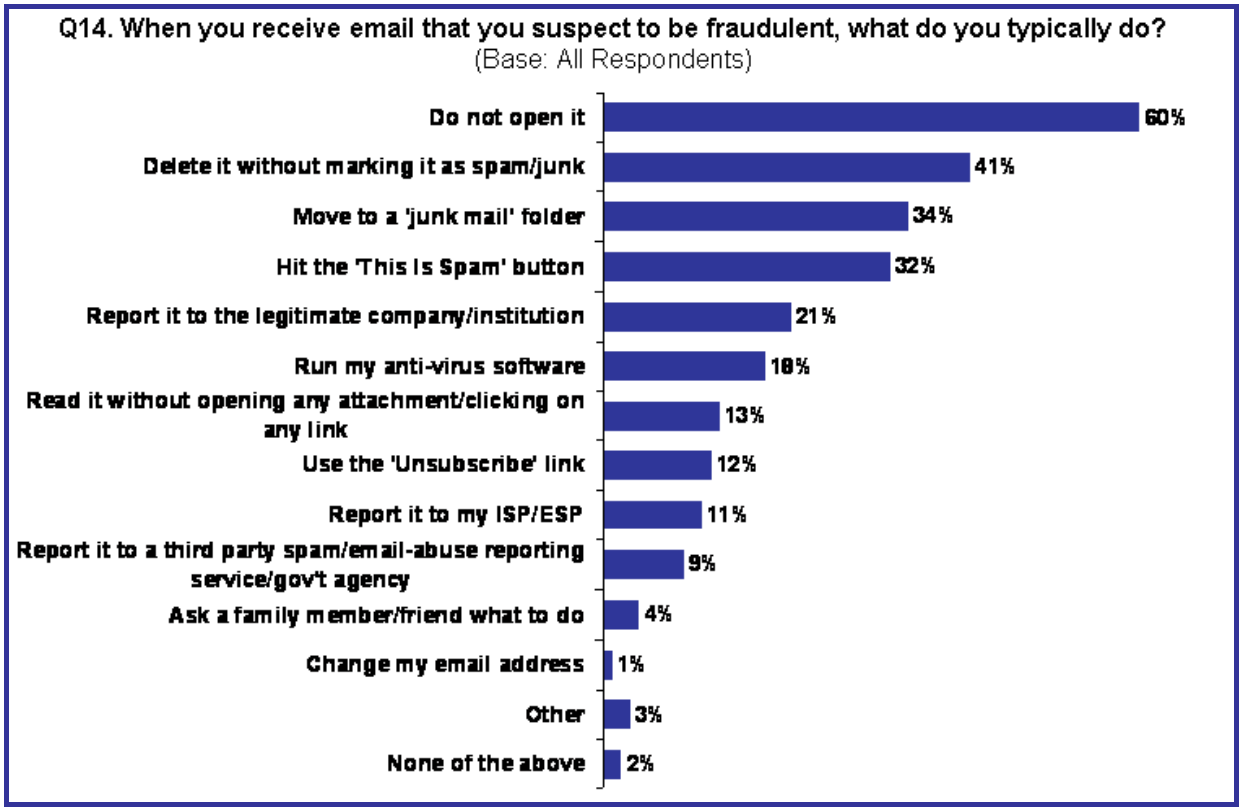
When email users receive messages that they think may be fraudulent (e.g., pretending to come from a bank or a merchant and asking for personal information), they tend to handle it much like the do spam.

Six in ten (60%) say that they typically do not open these suspicious messages, though they are more likely to delete it without flagging it (41%) than they are to move it to a junk folder (34%) or hit the spam button (32%).

At the same time, they are more likely to report fraudulent email than they are to report spam: 11% say that they usually report fraudulent email to their ISP or ESP and 9% to an email abuse reporting service or government agency. Additionally, one in five (21%) says that they frequently report fraudulent emails to the legitimate company or institution.

While 18% try to protect their computer by running their anti-virus software, nearly as many put read the message (but avoid clicking on links or attachments) (13%) or try to unsubscribe (12%).

Few typically ask a friend or family member what to do (4%) or change their email address (1%) when they receive an email they suspect is fraudulent.



Online respondents to the 2009 survey were most likely to say they delete email they suspect to be fraudulent (66%) or "mark it as spam and then delete it" (57%). Very few said that they reported it to the company (3%) or to their "ISP or email provider" (3%).

- Users in the U.S., followed by those in the U.K. and Canada, are more likely than their counterparts in France and Spain to say they usually report fraudulent emails, most commonly to the legitimate company or institution.
- Users in France are least likely to use the "spam" button (22%) yet are the most likely to move fraudulent emails to a junk mail folder (42%).
- How email users handle fraudulent email varies significantly by age and experience with Internet security issues. While roughly a third of users across all age groups say that they typically move these messages to a junk folder, adults under 55 are more likely than those who are older to flag these messages as spam (34% vs. 25%). Similarly, those aged 55 and older are most likely to just delete these emails without

flagging them first (46%). At the same time, those 55 and older are more likely than those under 35 to report it to the legitimate company (29% vs. 16%).

- Differences based on age may reflect the fact that older users tend to describe themselves as being less experienced than do younger users. Those who say they are experts or very experienced are more likely than those with little to no experience to say that they make use of the spam button (46% vs. 21%) and to move fraudulent emails to their junk folder (38% vs. 30%), while those with less experience tend to just delete these emails (46% vs. 36%). Also, those who are better versed are also more likely to notify the legitimate company about the fraudulent email (27% vs. 16%).

Risky Online Behavior

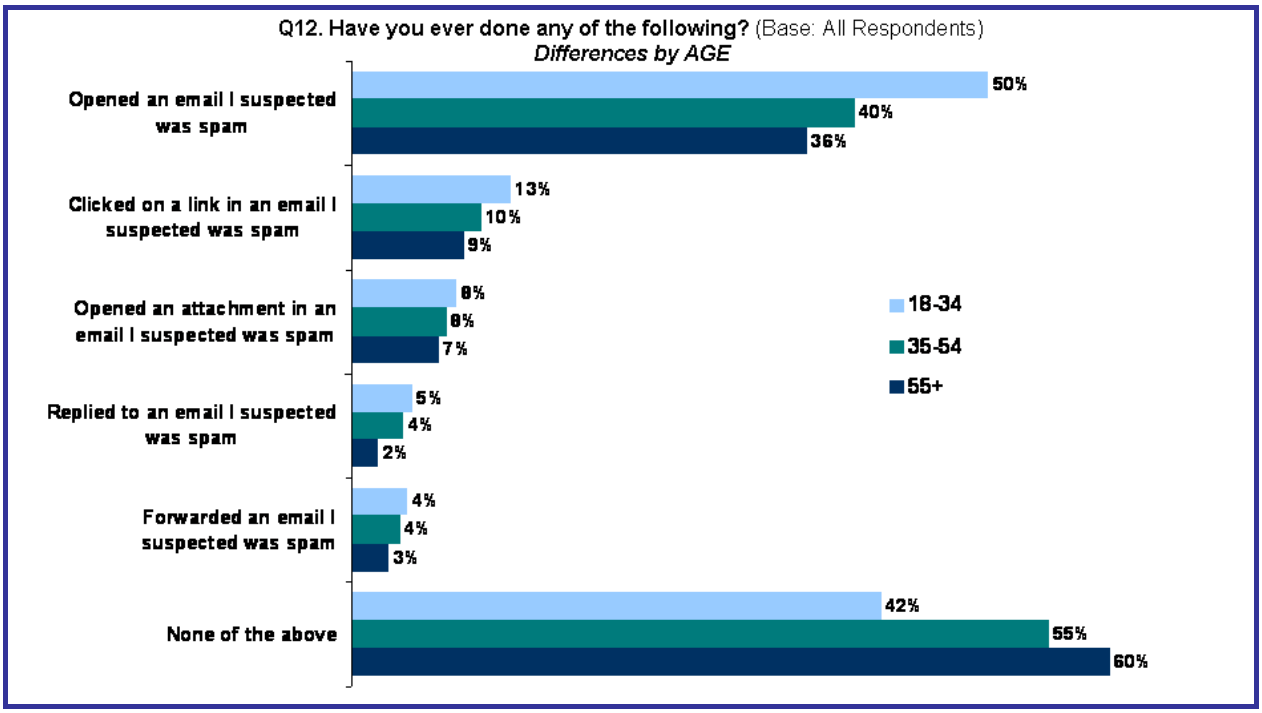
Though six in ten say that they typically do not open messages they think are spam, 43% of email users have opened spam in the past, and many have put themselves at even greater risk: clicking on links (11%), opening attachments (8%), replying (4%) or forwarding (4%) these messages.

While findings are fairly consistent across markets, a few differences do emerge:

- U.S. and Canadian users are more likely than those in Western Europe to report having replied to (6% vs. 3%) or forwarded (6% vs. 3%) emails that they suspected were spam.
- Email users in France are those least likely to say that they have opened spam (38%).

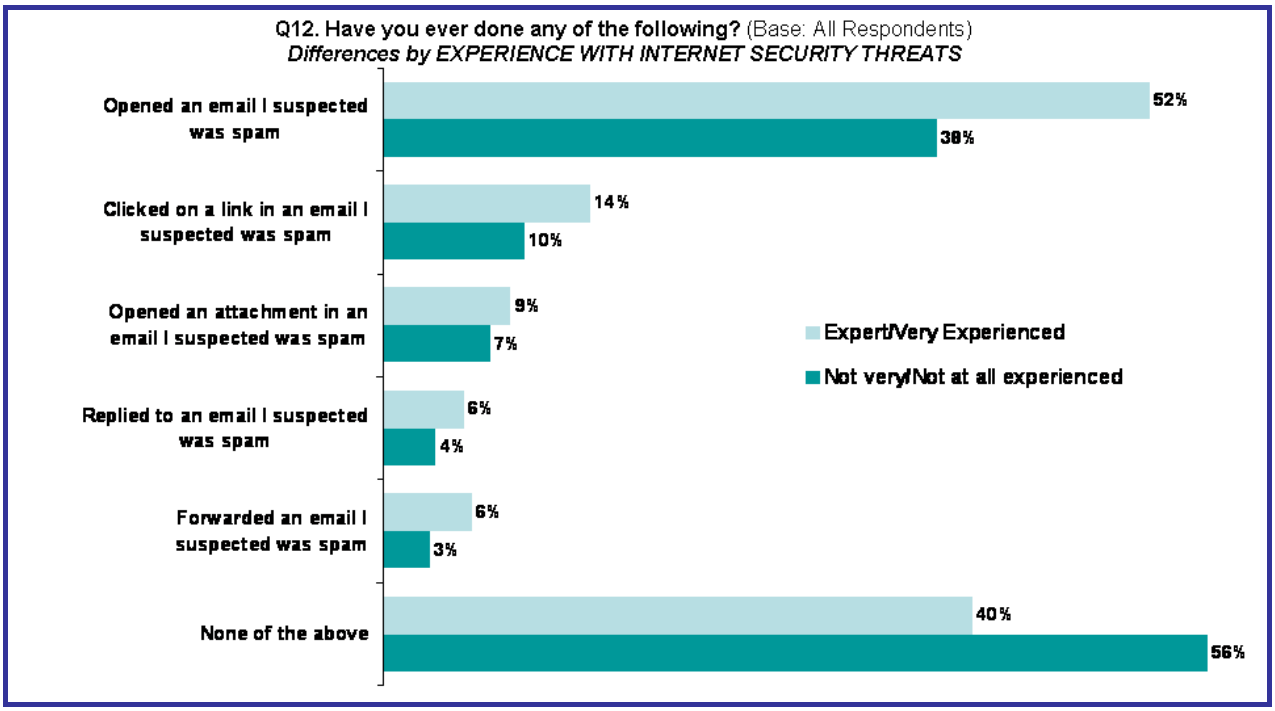
However, greater differences emerge across demographic groups, particularly gender and age, with men and younger email users being more likely to to put themselves at risk.

- Men are more likely than women not only to open spam (47% vs. 39%), but also to click on links (13% vs. 8%), to click on attachments (10% vs. 6%), and to reply to spam (5% vs. 3%).
- Email users under the age of 35 also tend to engage in riskier behavior while older users tend to be more cautious. They are more likely not only to open spam (50% 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).

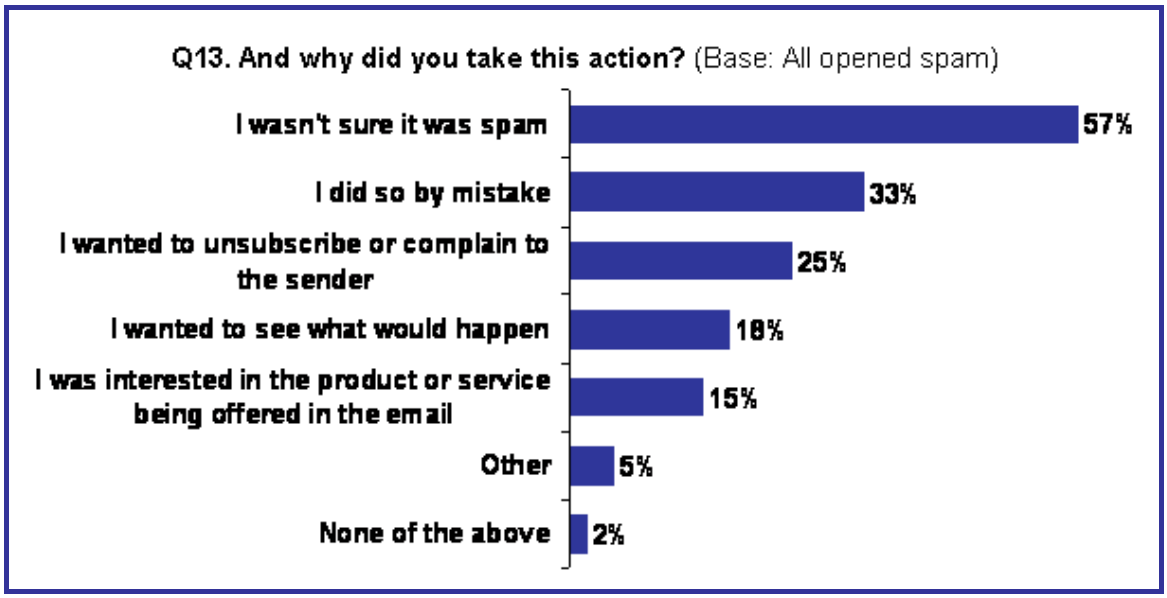


Those who have had a virus are more likely than those who have not to have opened spam in the past (48% vs. 37%).

Those who consider themselves experts or very experienced with Internet security – and who also tend to be younger – are more likely than those who feel inexperienced to have opened spam (52% vs. 38%).



While most users who have opened spam in the past say that it was because they didn't realize it was spam (57%) or they did so by mistake (33%), others have opened emails that they expected were spam intentionally. A quarter (25%) opened a suspicious email in an effort to unsubscribe, 18% just wanted to see what would happen, and 15% did so out of interest in the product or service being offered.

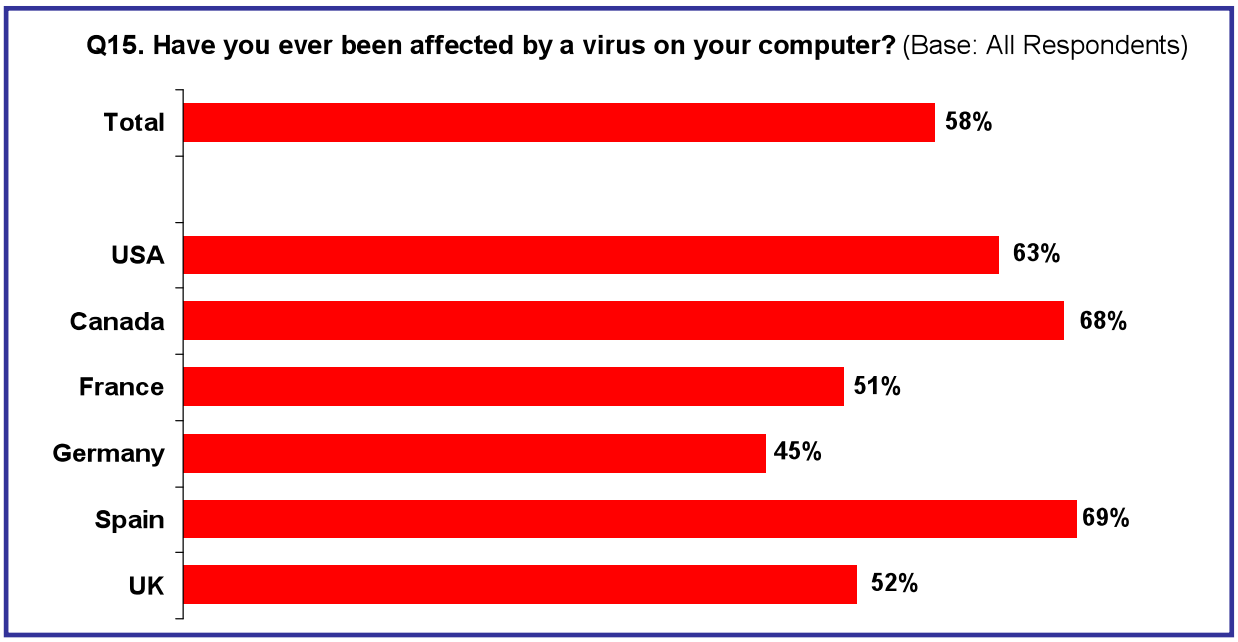


- Users in the U.S. are more likely than those in other countries to say that they opened spam in order to unsubscribe (35%) or to find out more about the products or services being offered (20%). Canadians tend to be more likely to say that they opened spam accidentally (40%), while those in Germany are most likely to have opened spam because they didn't realize that it was in fact spam (58%).
- Men – who also tend to take more risks when sorting through their inbox – are more likely than women to say they open spam purposefully, out of curiosity (21% vs. 14%) or out of interest in the email's offerings (17% vs. 13%).
- Users under 35 who have opened spam are also more likely than their older counterparts, especially those 55 and older, to have done so to see what would happen (21% vs. 12%). In contrast, those aged 55 and older who have opened spam are more likely than those who are younger to say that they did so because they were not sure that it was spam (66% vs. 53% of those under age 35).
- Majorities of email users across experience levels have trouble correctly identifying spam, with "experienced" users being nearly as likely as those with little to no experience to say that they opened these messages because they were not sure it was spam (53% vs. 59%).

The 2010 results are consistent with those from the 2009 U.S. survey when those who did click on spam (58%) said they either made a mistake, wanted to send a note to the company, were interested in the product or service, or were not sure why they did it.

6. Detailed Findings: Awareness, Concern about Bots Lagging

Although most users say they keep their anti-virus software updated, three in five (58%) report that their computer has been affected by a virus. Users in Spain and Canada are those most likely to have been infected.



Across demographic groups, those who tend to engage in riskier behavior when it comes to opening spam are also those most likely to have been infected with a virus: namely, men (61%), users under 35 (63%), and those who consider themselves to be experts or very experienced with Internet security (65%).

Among those who have had a virus, the most common course of action by far was running their anti-virus software (64%).

- Those most likely to have run their anti-virus software are users in the U.K. (72%) and Germany (71%). Users under 55 are more likely than those who are older to report having run their anti-virus software when their computer was infected (65% vs. 58%). Still, roughly six in ten across demographic groups say that this was the action that they took when they realized that they had a virus.

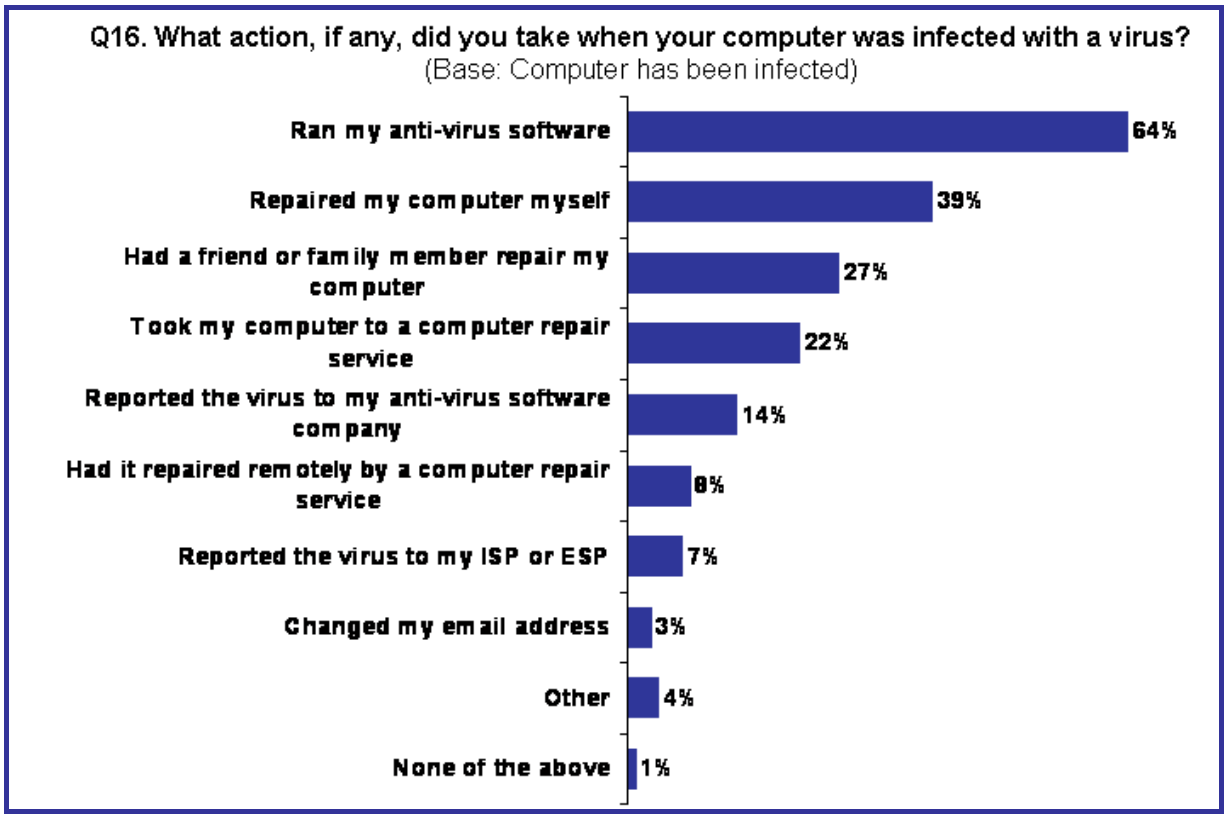
Four in ten (39%) say that when their computer was infected, they repaired their computer themselves while 27% enlisted the help of a friend or family member.

Less than a quarter (22%) took their computer to a repair service while 8% had it repaired remotely by a computer repair service.

- Canadians are more likely than others to say they used a repair service (32%).

Fewer reported the virus to their anti-virus software company (14%) or to their ISP or ESP (7%). Just 3% changed their email address while 4% took some other action when their computer became infected.

- Men are much more likely than are women to say that they repaired their computer themselves (49% vs. 26%) while women are more likely to seek the help of a friend or family member (35% vs. 20%).
- Younger users, particularly those under 35, are much more likely to take on the repairs themselves (47% vs. 19% of those aged 55 and older). These older users are more likely to get help from a loved one (33% vs. 25%) or a repair service (33% vs. 17%).
- Likewise, those who are experienced with Internet security are more likely to do it themselves (69% vs. 15%) while those with limited experience tend to rely more on friends or family (40% vs. 12%) or a repair service (29% vs. 13%). Experienced users are also more likely to run their anti-virus software (73% vs. 53%).

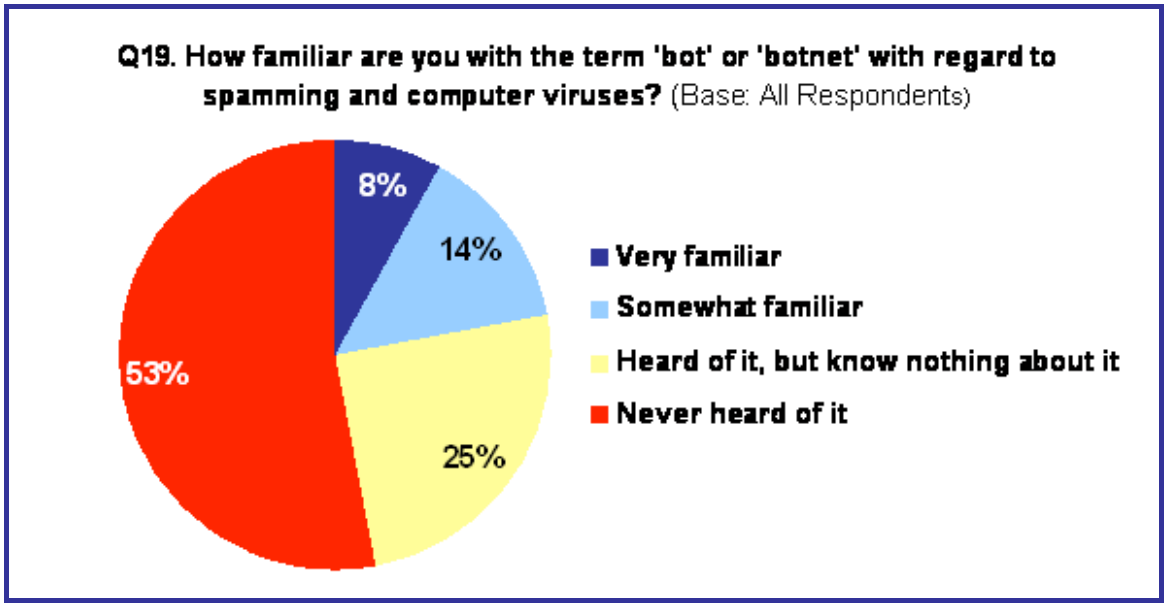


Lack of Familiarity and Concern about Bots

Though a majority of email users have been infected with a computer virus, the survey findings point to lacking awareness of bots and botnets.

More than half of all users across the six countries surveyed (53%) have never heard of the term "bot" or "botnet", and an additional 25% say that although they have heard the term, they know nothing about it. Just one in five (22%) are at least somewhat familiar with "bots."

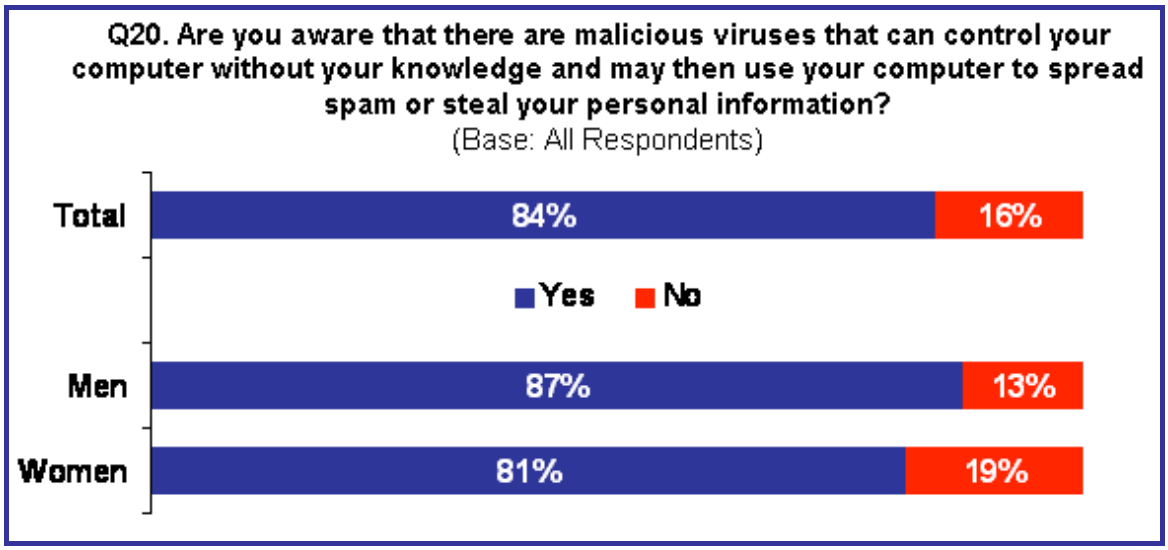
- Those least likely to be aware of the term "bot" or "botnet" include women (only 38% have heard of it vs. 56% of men), users aged 55 and older (36%) and those who are not very/not at all experienced with Internet security (only 22%).
- Users in Germany (57%) and in English-speaking countries are more likely to have heard of the term than those in France (36%) and Spain (37%).



While 84% have heard of the *concept* of bots, presented as "malicious viruses that can control your computer without your knowledge and may then use your computer to spread spam or steal your personal information," 16% of respondents, representing tens of millions of men and women across the six countries, say they are not aware of them.

- Again, awareness of the concept of bots is highest in Germany (91%), but varies little across the other five markets.
- Across demographic groups, men are more likely to have heard of these viruses than are women (87% vs. 81%), though there are no significant differences across age groups.
- Those who describe themselves as experts or very experienced when it comes to Internet security are much more likely to be aware of the concept of bots than are those with little or no experience (96% vs. 73%).

In the U.S. at 82%, awareness of the bot concept is five points higher in the 2010 survey than it was among online respondents of the 2009 survey.

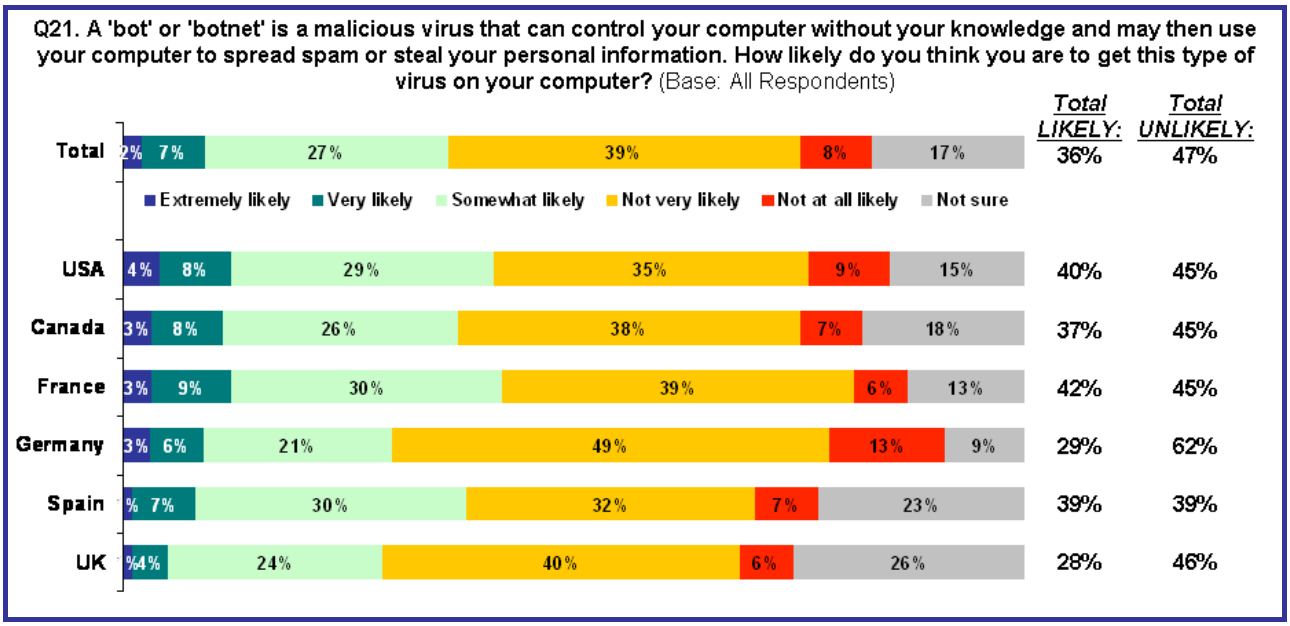


Despite the prevalence of viruses, just 9% think that it is very or extremely likely that their computer will become infected. Rather, nearly half (47%) say this is not very or not at all likely. Roughly a quarter (27%) thinks it is somewhat likely while 17% are unsure.

- Even among those who have had a virus in the past, more than four in ten do not expect that their computer will be infected by a bot: 43% of them say it is not very or not at all likely, compared with 53% of those who say their computer was never infected by a virus.
- Email users who view themselves as experienced tend to be more confident than those with little or no experience with Internet security that they will be spared from getting a bot (63% not very or not at all likely vs. 36%).
- German users – many of whom view themselves as experienced and who are also less likely than others to have been infected by a virus in the past – are particularly prone to thinking they are immune from bots: Six in ten (62%) say they are not very or not at all likely to get one. British and Spanish users are more likely than others to say they are unsure (26% and 23%, respectively).

Those who have opened spam in the past feel no more vulnerable than do those who have avoided opening these emails (48% unlikely vs. 46%).

The findings here very much align with those from last year's U.S. survey when eight out of ten respondents said they are aware of malicious viruses that can control their computer, yet few believed they were susceptible to getting such a virus. Using a scale of 1 to 5, with 5 meaning extremely likely and 1 meaning not at all likely, 43% of respondents selected a 1 or a 2, indicating that they think they are not very or not at all likely to get a bot on their computer. Similarly, 45% of U.S respondents in the 2010 study say that they are not very or not at all likely to get a bot.



Recognizing Bots

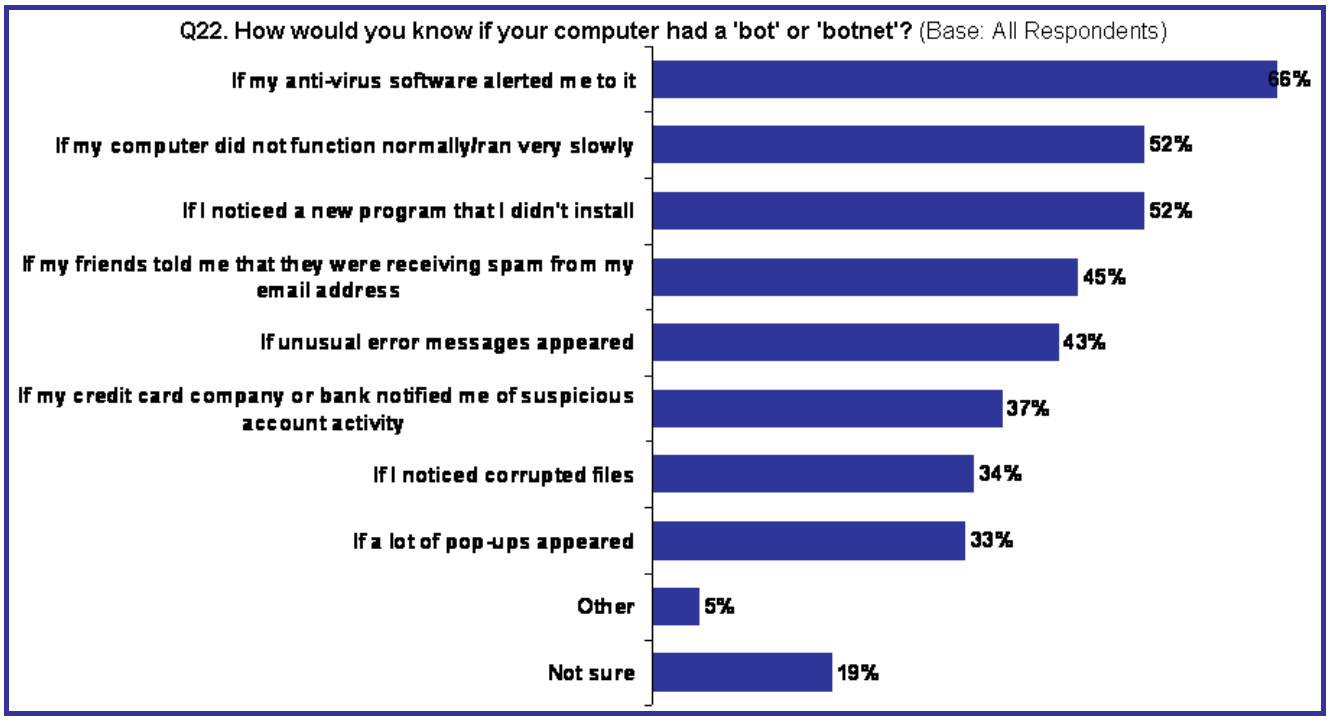
*If they were to become infected with a bot, email users are most likely to say they would r*ely on their anti-virus software to alert them (66%). Majorities also say that they would know that they have a bot if their computer wasn't functioning normally or was running slowly (52%) or if they noticed a program that they hadn't installed (52%).

More than four in ten say that they would know that they had a bot if their friends told them that they had been receiving spam from their email address (45%) or if unusual error messages appeared (43%).

Roughly a third would recognize that their computer had a bot if their credit card company or bank notified them of suspicious account activity (37%), if they noticed corrupted files (34%), or if a lot of pop-ups appeared (33%). One in twenty (5%) would look for other indicators. However, nearly one in five (19%) say that they are unsure as to how they would recognize a bot.

- Over half of users in Canada (51%) and France (53%) say that they would recognize that they had a bot if their friends told them that they were receiving spam from their email address. A majority (56%) of Germans would look out for unusual error messages while users in Spain are most likely to be unsure as to how to recognize a bot (28%).
- Users aged 55 and older – who are also those most likely to keep their anti-virus software updated – would be more likely than those under 35 to rely on an alert from their anti-virus software (70% vs. 63%).
- For each possible indicator, "experienced" users are more likely than inexperienced ones to say they would rely on it to recognize that they have a bot overall. Hence, 28% of those with little to no experience with Internet security threats say that they are not sure how they would recognize a bot on their computer compared with just 6% of experienced users.
- Women are also more likely than men to say they would be unsure (22% vs. 15%).

- Understandably, many who were not aware of the concept of bots are unsure as to how to recognize them (39%).



7. Detailed Findings: Whose Responsibility Is It to Stop Bots?

Email users primarily look to Internet and email service providers as those most responsible for stopping the spread of computer viruses, fraudulent email, spyware, and spam (65%), followed by anti-virus software companies (54%).

Less than half (48%) hold themselves accountable for stopping the spread of viruses and spam, though fewer hold other groups and organizations responsible: leading computer software companies (37%), the government/consumer protection agencies (35%), social networking sites (22%), computer manufacturers (20%), computer and software retailers (19%), consumer advocacy groups (15%), and professional associations (12%).

- Users in the U.S., Canada and the U.K. tend to have higher expectations than do their counterparts in continental Europe with regard to the responsibility of most stakeholders cited.
- Older email users also tend to be more likely than younger users to hold a variety of businesses and organizations accountable, particularly ISPs and ESPs and anti-virus software companies. At the same time, they are also most likely to put the responsibility on themselves.

Q17. Who do you feel should be most responsible for stopping the spreading of computer viruses, fraudulent email, spyware, and spam? (Base: All Respondents)

	Age		
	18-34	35-54	55+
Internet and email service providers	57%	67%	77%
Anti-virus software companies	52%	54%	62%
Myself	45%	49%	51%
Leading computer software companies	34%	38%	43%
The government/consumer protection agencies	33%	35%	36%
Social networking sites	23%	22%	22%
Computer manufacturers	18%	22%	23%
Computer and software retailers	18%	20%	20%
Consumer advocacy groups	14%	14%	18%
Professional associations	13%	12%	11%
Other	5%	5%	2%

- Those who consider themselves to be experts or very experienced in regard to Internet security concerns are more likely to personally assume responsibility for stopping the spread of viruses than are those who are less experienced (62% vs. 38%).

While users are most likely to hold ISPs and ESP responsible for stopping bots, many more give good ratings to anti-virus software companies for stopping viruses (67% very/fairly good) than do to ISPs/ESPs (41%), perhaps because they are less aware of the steps ISPs and ESPs are taking to protect them.

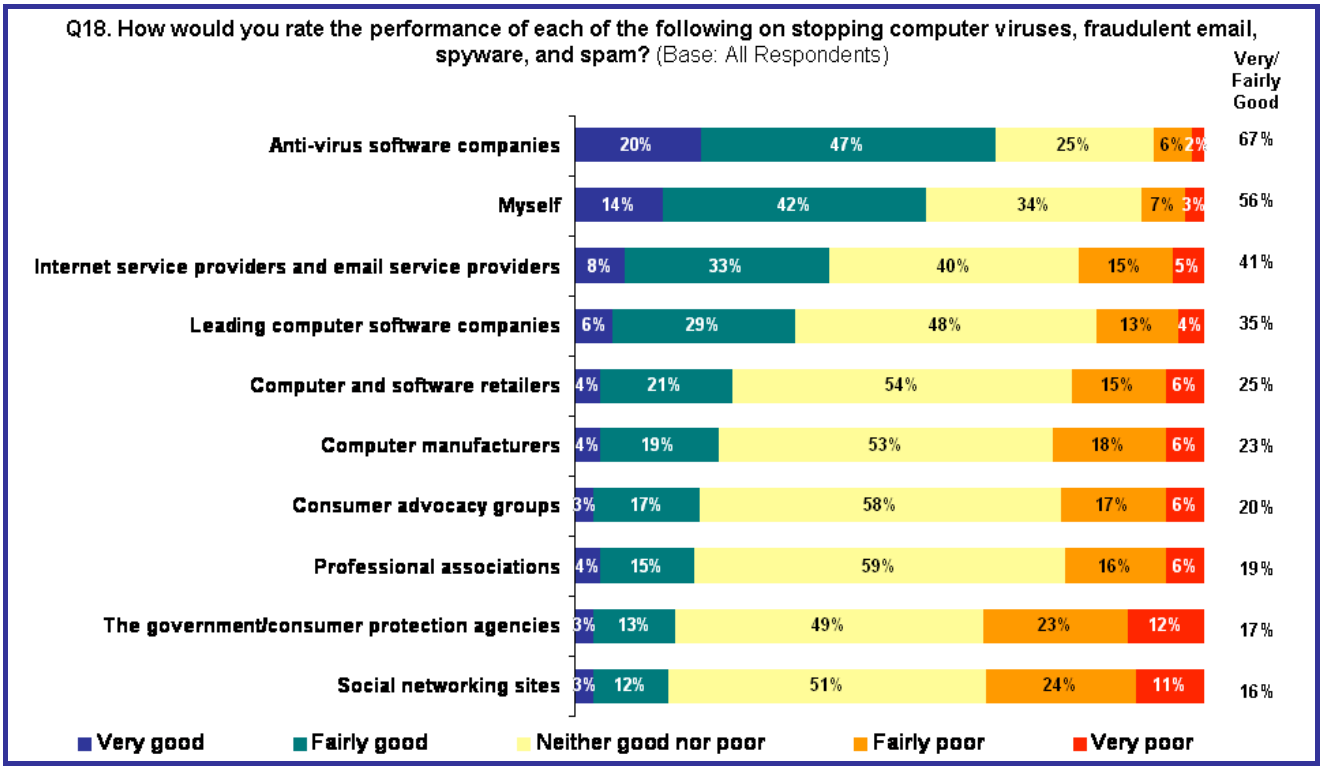
Despite the fact that less than half (48%) hold themselves accountable for stopping the spread of viruses and spam, a majority (56%) rate themselves as being very or fairly good at stopping viruses and spam.

Anti-virus software companies and users themselves get poor ratings from just one in ten respondents, while nearly all other entities get poor ratings from at least two in ten respondents.

ISPs and ESPs and computer software companies get positive ratings (41% and 35%, respectively) from about twice as many users as they get poor ratings.

Organizations in the next tier get about as many good ratings as they get poor ratings – computer and software retailers, computer manufacturers, consumer advocacy groups and professional associations.

Finally, many more are critical of social networking sites and of the government and consumer protection agencies than have a positive assessment of their performance in stopping computer viruses, fraudulent email, spyware, and spam.



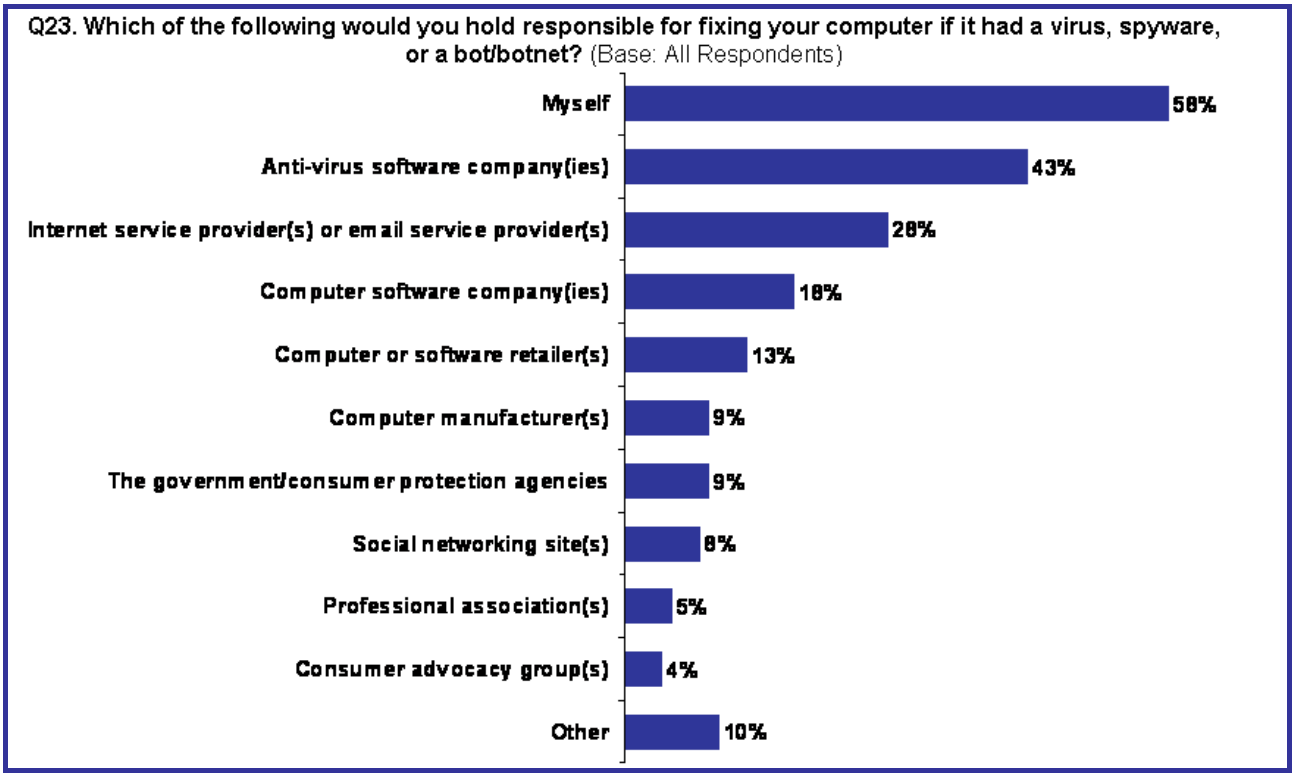
- Users in the U.S., U.K. and Canada tend to give each of the stakeholders cited better marks than do those in France and Spain, particularly when it comes to anti-virus software companies and ISPs/ESPs.
- Those with more experience with Internet security also tend to award better ratings across the board than do those with less experience. They are especially prone to be satisfied with their own performance in stopping viruses and fraudulent email as 78% rate is a good. In contrast, only 38% of those with little or no experience rate their performance as good.
- Users aged 55 and older are not only more likely than younger users to hold anti-virus companies responsible for stopping bots, but they are also most likely to think that they are doing a good job at it (74% vs. 65% of those aged 18-34).

In a differently-worded question in the 2009 survey, "virus protection software" and "retailers" were rated best when it comes to stopping the creation of computer viruses, fraudulent email, spyware, and spam. Respondents were not asked to rate themselves.

Whose Responsibility Is It to Fix Infected Computers?

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%).

Fewer would hold computer software companies (18%), computer or software retailers (13%), computer manufacturers (9%), the government/consumer protection agencies (9%), social networking sites (8%), professional associations (5%) or consumer advocacy groups (4%) responsible for fixing their computer if it were to be infected with a virus, spyware or bot. One in ten (10%) would hold some other party accountable.



- Those with a good deal of experience with Internet security are much more likely to hold themselves responsible than are those with little to no experience (70% vs. 49%), while inexperienced users tend to be more likely to hold third parties accountable – particularly anti-virus companies and ISPs and ESPs.
- Looking across the six countries, holding oneself responsible is more prevalent in the U.K. (73%), Canada (66%), and the U.S. (65%).
- French users, who are much more likely than their counterparts in other countries to describe themselves as inexperienced when it comes to Internet security, are particularly prone to place responsibility on anti-virus software companies (53%) and are less likely to place the responsibility on their own shoulders (42%). German (39%)

and French (40%) users are also more likely than others to hold their ISP or ESP responsible for fixing their computer if it were to become infected.

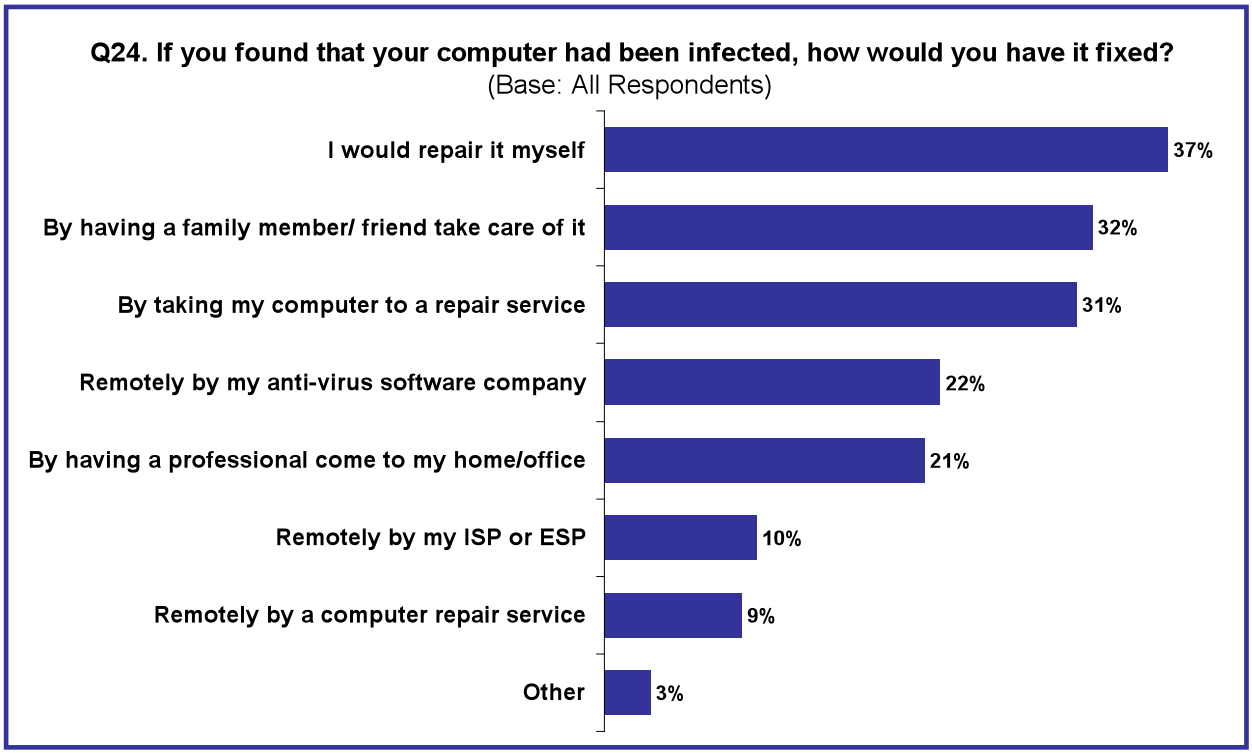
- Again, older users are more likely to hold a variety of parties responsible When it comes to fixing their infected computer, significantly greater proportions of those aged 55 and older than of those under the age of 35 hold anti-virus companies (48% vs. 42%) and ISPs and ESPs (37% vs. 27%) responsible.

The survey findings are consistent with those of the 2009 U.S. study when 52% of online respondents said that they would hold themselves accountable, followed by anti-virus software companies (28%) and computer repair professionals (27%).

Repairing Infected Computers

When it comes to having their infected computer repaired, users are most likely to say that they would repair it themselves (36%), have a friend or family member take care of it (32%), or take it to a repair service (31%). However, notable differences emerge across countries.

- Users are most likely to say that they would take their computer to a repair service in Canada (43%) and in Spain (42%). In the U.S., users are roughly equally as likely to look to a repair service (35%) as to fixing their computer themselves (34%). Self-repair would be most common in Germany (44%) and in the U.K. (36%), while French users are most likely to enlist the help of a friend or family member (42%).
- Respondents in the U.S. (40%), followed by those in the U.K. (36%), are most likely to mention having their computer repaired remotely, either by their anti-virus software company, their ISP or ESP, or by a computer repair service. In contrast, users in Spain (21%) and Germany (24%) would be least likely to take advantage of these services.



Generally those who are more likely to hold themselves responsible for fixing their infected computer are also most likely to say that they would handle the repair themselves.

- Men are more likely than women to both hold themselves responsible for fixing their computers (61% vs. 55%) and to say that they would repair it themselves (47% vs. 24%). Women tend to say they would turn to a friend or family member to take care of it (41% vs. 24%).
- Younger users are also more likely to take it upon themselves (18-34: 45%; 35-54: 36%; 55+: 20%).
- Experienced users are five times more likely than those with little or no experience with Internet security to say they would tackle the repairs themselves (73% vs. 14%).

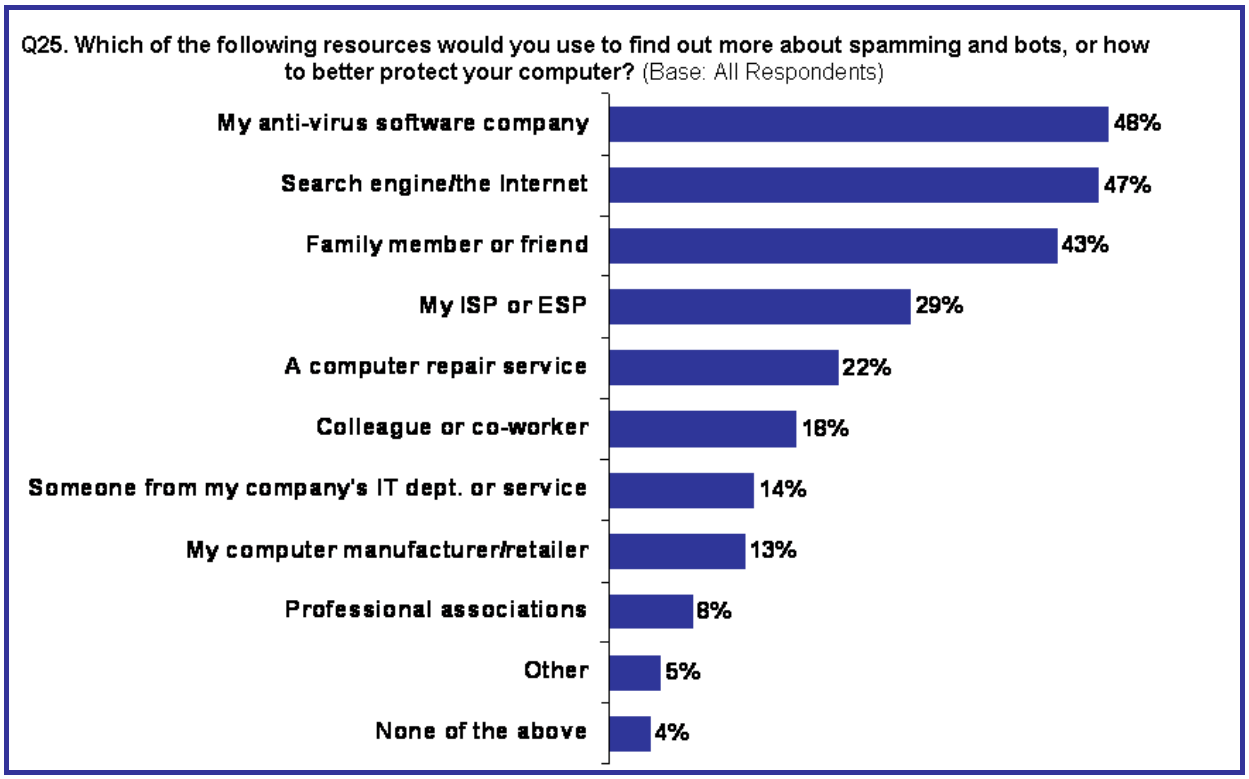
The 2009 study similarly showed that while self-repair is most common, those with greater experience are more likely than those who are inexperienced to take on this task.

Where Users Go to Find Out More about Security Threats

Again users display much reliance on anti-virus software when it comes to Internet security, as it is the resource they are most likely to turn to in order to learn how to better protect their computer (48%) along with online search engines (47%) and family members and friends (43%).

Roughly a quarter say they would rely on their ISP or ESP (29%) or a computer repair service (22%). Fewer would turn to a colleague or co-worker (18%), someone from their

company's IT department (14%), their computer manufacturer or retailer (13%), or a professional association (8%).



- Email users in the U.S. and U.K. (58% in both countries) are most likely to view their anti-virus software company as a resource in this regard, though just 34% of French users feel this way. Rather, French users are more likely to look to a family member or friend (51%) or the Internet (49%) for information.
- Half of men would utilize their anti-virus company (51%) or search the Internet (50%) to find out more about protecting their computer while half of women would ask a relative or friend (51%).
- Users 35 and over are most likely to look to their anti-virus company (51%) while younger users are most likely to go online (49%). These younger users are much more hesitant than older users to seek information from their ISP or ESP (20% vs. 34%).
- Looking at experience levels, those who are well versed in Internet security matters are more much more likely than those who are not to look for information from their anti-virus software company (54% vs. 40%) or search for it online (62% vs. 34%) while those with less experience are much more likely to rely on a relative or friend (55% vs. 30%) or on a computer repair service (26% vs. 16%).

8. Demographics and Classification Variables

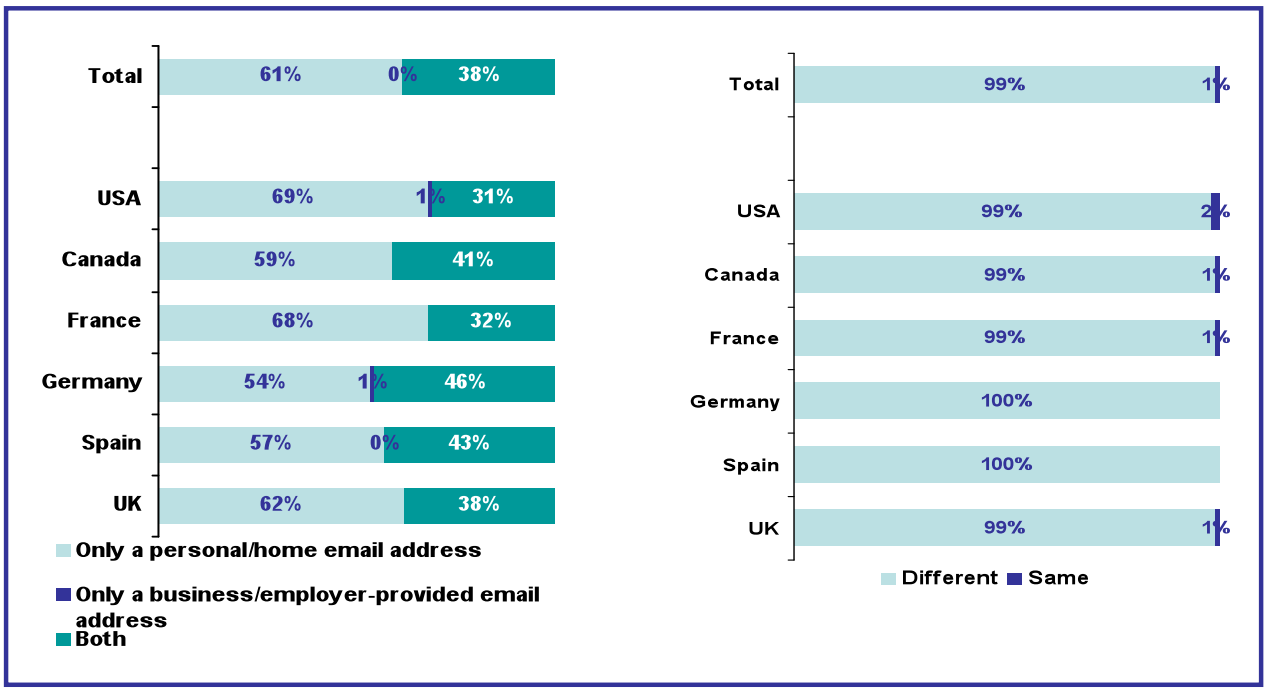
Operating System

Q26. What type of operating system does your personal computer have? (Base: All Respondents)

	Total	USA	Canada	France	Germany	Spain	UK
Windows (any version)	**93%**	89%	91%	94%	94%	94%	95%
Mac (any version)	**5%**	7%	6%	4%	4%	3%	3%
Linux (any version)	**1%**	0%	0%	1%	2%	2%	0%
Other	**1%**	1%	1%	0%	0%	0%	0%
Not sure	**1%**	3%	1%	1%	1%	1%	1%

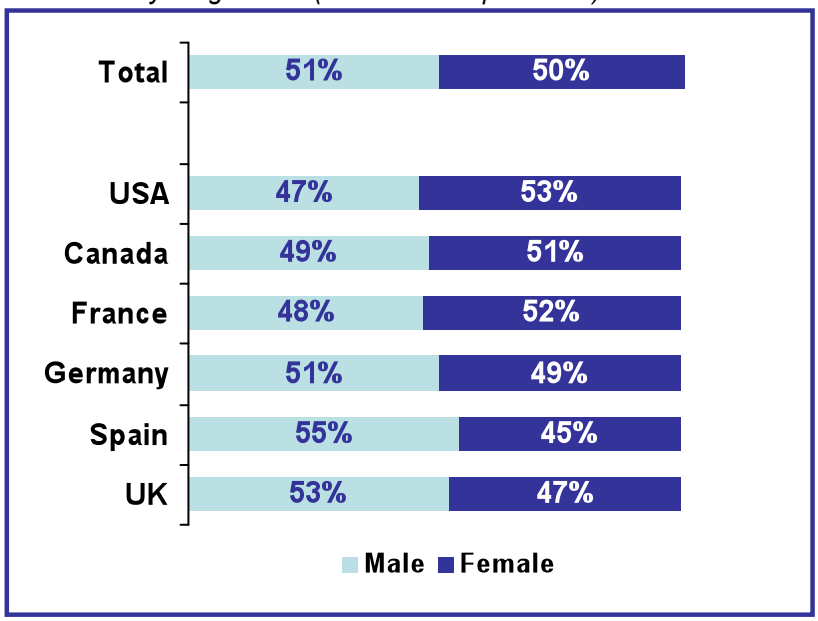
Type of Email Address

Q2. Do you have only a personal/home email address, only a business/employer-provided email address, or both? (Base: All Respondents)
Q3. Are they different email addresses or the same one? (Base: Answered "both" in Q2)



Gender

S1. What is your gender? (Base: All Respondents)



Age

S2. What is your age? (Base: All Respondents)

	Total	USA	Canada	France	Germany	Spain	UK
18 to 24	**17%**	16%	14%	19%	17%	20%	14%
25 to 34	**23%**	20%	21%	24%	20%	31%	19%
35 to 44	**24%**	20%	25%	24%	26%	25%	25%
45 to 54	**19%**	20%	21%	18%	21%	15%	20%
55 to 64	**12%**	15%	11%	12%	11%	7%	16%
65 or older	**6%**	9%	8%	3%	5%	2%	6%
18 to 34	**39%**	36%	35%	43%	37%	51%	33%
35 to 54	**43%**	40%	46%	42%	47%	40%	45%
55+	**18%**	24%	19%	15%	16%	9%	22%

Employment Status

Q27. What is your employment status or profession? (Base: All Respondents)

	Total	USA	Canada	France	Germany	Spain	UK
Self employed	**8%**	8%	9%	5%	9%	10%	6%
Employed full-time	**44%**	37%	42%	52%	44%	45%	45%
Employed part-time	**9%**	10%	12%	10%	8%	7%	9%
Retired	**11%**	12%	13%	10%	11%	4%	16%
Homemaker	**6%**	10%	6%	5%	5%	3%	4%
Unemployed	**11%**	12%	8%	7%	9%	17%	11%
Student	**9%**	8%	8%	10%	13%	13%	6%
Other	**2%**	3%	2%	2%	1%	1%	2%

Education

S3. What is the highest level of formal education that you have completed? (Base: All Respondents)

U.S.	
Grade school or some high school	4%
Completed high school	34%
Some college but did not finish	36%
Completed a two year college degree	6%
Completed a four year college degree	13%
Completed a post-graduate degree such as a Master's or Ph.D.	7%
HS or less (Low)	38%
Some college (Middle)	36%
College grad + (High)	26%

Canada	
Grade school or some high school	9%
Complete high school	27%
Complete technical or trade school/Community college	18%
Some community college or university, but did not finish	28%
Complete university degree, such as a Bachelor's	15%
Post-graduate degree, such as a Master's or Ph.D.	4%
HS or less (Low)	35%
Post Secondary (Middle)	46%
University (High)	19%

France	
No diploma	6%
BEP/CAP	14%
Middle school certificate	16%
High school diploma or equivalent	34%
2 years of college (DEUG)	12%
3 years of college (License)	6%
4 or more years of college (Master's or higher)	11%
Low	22%
Middle	48%
High	30%

Germany	
Secondary general school without completed vocational training	3%
Secondary general school with completed vocational training	6%
Intermediate school , grammar school without university qualification exam	11%
University qualification exam	55%
Tertiary Education, e.g. university, technical college	25%
Low	20%
Middle	55%
High	25%

Spain	
None/Incomplete Primary	1%
Primary (Elementary) Completed	6%
Secondary (Jr. High) Completed	18%
Secondary (High School) Completed -Vocational Training	30%
University Mid Level	22%
University Superior Level	20%
Post Graduate / Doctors	4%
Low	25%
Middle	30%
High	45%

U.K.	
None/left with no qualifications	11%
GCSE/O Levels/CSE	24%
A Levels/BTEC/HND/other post-16 qualification	30%
First Degree	28%
Second Degree (MA/MSC/MPhil etc)	6%
Doctorate	1%
Low	35%
Middle	30%
High	35%

9. Appendix: Questionnaires

English (US, Canada, UK)

S1. What is your gender?

Male
Female

S2. What is your age?

18 to 24
25 to 34
35 to 44
45 to 54
55 to 64
65 or older

S3. EDUCATION:

[UNITED STATES]
What is the highest level of formal education that you have completed?

Grade school or some high school
Completed high school
Some college but did not finish
Completed a two year college degree
Completed a four year college degree
Completed a post-graduate degree such as a Master's or Ph.D.

[CANADA]
What is the highest level of formal education that you have completed?

Grade school or some high school
Complete high school
Complete technical or trade school/Community college
Some community college or university, but did not finish
Complete university degree, such as a Bachelor's
Post-graduate degree, such as a Master's or Ph.D.

[UK]
What is the highest level of formal education that you have completed?

None/left with no qualifications
GCSE/O Levels/CSE
A Levels/BTEC/HND/other post-16 qualification
First Degree
Second Degree (MA/MSC/MPhil etc)
Doctorate

1. How would you describe yourself when it comes to your experience with security on the Internet, including firewalls, spam, junk mail and computer viruses?

   [REVERSE SCALE ON ½ SAMPLE]
   An expert
   Very experienced
   Somewhat experienced
   Not very experienced
   Not at all experienced

2. Do you have only a personal/home email address, only a business/employer-provided email address, or both? [Single response]

   Only a personal/home email address
   Only a business/employer-provided email address
   Both

   [ASK IF BOTH IN Q2]
3. Are they different email addresses or the same one?

   Different
   Same

   [ASK IF "BUSINESS/EMPLOYER-PROVIDED EMAIL ADDRESS ONLY" IN Q2 OR "SAME" IN Q3]
4. Does your business/employer have an IT service, department or a person other than yourself who manages the security of your business/employer-provided email address?

   Yes [TERMINATE]
   No
5. In general, how important do you consider each of the following types of personal email sent to you?

   ITEMS [Randomize]
   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 [anchor]

   SCALE:
   Extremely important
   Very important
   Somewhat important
   Not very important
   Not important at all

6. Which of the following most applies to the computer you use most often for your personal email? [Single response]

I personally update the anti-virus software when needed
Someone else updates the anti-virus software when needed
Nobody updates the anti-virus software
The anti-virus software updates itself automatically
There is no anti-virus software on this computer
Not sure

[ASK IF "NOBODY UPDATES THE ANTI-VIRUS SOFTWARE" IN Q6]

7. Which of the following reasons best describes why your anti-virus software is not updated? [Single response]

[Randomize]
Unsure about how to update it
It doesn't need to be updated
I have never been prompted to update it
Not enough time/put it off until later
Too expensive
Never get a virus
None of these [anchor]

8. How do you personally define spam? Please select all that apply.

[Randomize]
Email I did not request
Email that I once requested, but no longer want
Email from porn, pills, body part enlargement, online casinos, etc.
Email that contains a virus or 'phishing' scheme
Email that violates anti-spamming regulations
Email in my spam or junk mail folder
Email from sources that I cannot 'unsubscribe' from
Jokes and silly messages forwarded to me
Other [anchor]

9. What actions, if any, have you taken to keep your personal email inbox free of spam? Please select all that apply.

[Randomize]
Installed a spam or junk mail filter
Added senders I recognize to my address book
Moved emails that I did not want from my inbox to my junk/spam folder
Used a separate email address when spam might occur
Avoided posting my email address on websites
Avoided giving out my email address
Set up an unusual email address that is hard to guess
Used a separate email address for friends and family
Other [anchor]
None of the above [anchor]

10. When going through your email box and deciding what email is spam and what is legitimate, what indicators do you rely on to help you decide? Please select all that apply

[Randomize]
The sender's name or address
The receiver's name or address
The subject line
The time of day/night when it was sent
The icons or other visual indicators that appear in my inbox beside the message
The content of the email
Spelling mistakes/poor grammar
Unusual language
Other [anchor]
I want all the email I receive [anchor]
None of the above [anchor]

11. When you receive email that you think is spam, what do you usually do? Please select all that apply.

[Randomize]
Hit the "This Is Spam" button
Move to a "junk mail" folder
Delete it without marking it as spam or junk
Do not open it
Read it without opening any attachment or clicking on any link
Report it to my Internet service provider or email service provider
Report it to a third party spam/email-abuse reporting service (e.g., SpamCop, Abuse.net) or a government agency
Change my email address
Use the "Unsubscribe" link
Other [anchor]
None of the above [anchor]

12. Have you ever done any of the following? Please select all that apply.

[Randomize]
Opened an email I suspected was spam [anchor]
Clicked on a link in an email I suspected was spam
Opened an attachment in an email I suspected was spam
Forwarded an email I suspected was spam
Replied to an email I suspected was spam
None of the above [anchor]

[Ask if anything but "none of the above" in Q12]

13. And why did you take this action? Please select all that apply.

[Randomize]
I was interested in the product or service being offered in the email
I wanted to see what would happen
I did so by mistake
I wanted to unsubscribe or complain to the sender
I wasn't sure it was spam
Other [anchor]
None of the above [anchor]

14. When you receive email that you suspect to be fraudulent (e.g., pretending to come from a bank or a merchant and asking for personal information), what do you typically do? Please select all that apply.

[Randomize]
Hit the "This Is Spam" button
Move to a "junk mail" folder
Delete it without marking it as spam or junk
Do not open it
Read it without opening any attachment or clicking on any link
Report it to my Internet service provider or email service provider
Report it to a third party spam/email-abuse reporting service (e.g., SpamCop, Abuse.net) or a government agency
Change my email address
Use the "Unsubscribe" link
Report it to the legitimate company or institution (e.g., my bank)
Run my anti-virus software
Ask a family member or a friend what to do
Other [anchor]
None of the above [anchor]

15. Have you ever been affected by a virus on your computer?

Yes
No

[ASK IF 'YES' IN Q15]

16. What action, if any, did you take when your computer was infected with a virus? Please select all that apply.

[Randomize]
Reported the virus to my Internet service provider or my email service provider
Reported the virus to my anti-virus software company (e.g., AVG, McAfee, Norton/Symantec, etc.)
Changed my email address
Had it repaired remotely by a computer repair service
Took my computer to a computer repair service
Repaired my computer myself
Had a friend or family member repair my computer
Ran my anti-virus software
Other [anchor]
None of the above [anchor]

17. Who do you feel should be most responsible for stopping the spreading of computer viruses, fraudulent email, spyware, and spam? Please select all that apply.

[Randomize]
Myself
The government/consumer protection agencies
Internet service providers and email service providers
Computer and software retailers
Professional associations
Leading computer software companies
Computer manufacturers
Anti-virus software companies
Social networking sites
Consumer advocacy groups
Other [anchor]

18. How would you rate the performance of each of the following on stopping computer viruses, fraudulent email, spyware, and spam?

[Same order as Q17]
Myself
The government/consumer protection agencies
Internet service providers and email service providers
Computer and software retailers
Professional associations
Leading computer software companies
Computer manufacturers
Anti-virus software companies
Social networking sites
Consumer advocacy groups

Scale:
Very good
Fairly good
Neither good nor poor
Fairly poor
Very poor

19. How familiar are you with the term "bot" or "botnet" with regard to spamming and computer viruses? [single response]

Very familiar
Somewhat familiar
Heard of it, but know nothing about it
Never heard of it

20. Are you aware that there are malicious viruses that can control your computer without your knowledge and may then use your computer to spread spam or steal your personal information?

Yes
No

21. 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?

[REVERSE SCALE ON ½ SAMPLE]
Extremely likely
Very likely
Somewhat likely
Not very likely
Not at all likely
Not sure [anchor]

22. How would you know if your computer had a "bot" or "botnet"? Please select all that apply.

[Randomize]
If my friends told me that they were receiving spam from my email address
If my credit card company or bank notified me of suspicious activity on my account
If my anti-virus software alerted me to it
If my computer did not function normally or ran very slowly
If unusual error messages appeared
If I noticed corrupted files
If I noticed a new program that I didn't install
If a lot of pop-ups appeared
Other [anchor]
Not sure [anchor]

23. Which of the following would you hold responsible for fixing your computer if it had a virus, spyware, or a bot/botnet? Please select all that apply.

[Same order as Q17]
Myself
The government/consumer protection agencies
Internet service provider(s) or email service provider(s)
Computer or software retailer(s)
Professional association(s)
Computer software company(ies)
Computer manufacturer(s)
Anti-virus software company(ies)
Social networking site(s)
Consumer advocacy group(s)
Other [anchor]

24. If you found that your computer had been infected, how would you have it fixed? Please select all that apply.

[RANDOMIZE]
Remotely by my Internet service provider or email service provider
Remotely by a computer repair service
Remotely by my anti-virus software company
By having a family member or a friend take care of it
By having a professional come to my home or office to repair
By taking my computer to a repair service
I would repair it myself
Other [anchor]

25. Which of the following resources would you use to find out more about spamming and bots, or how to better protect your computer? Please select all that apply.

[RANDOMIZE]
My Internet service provider or email service provider
My anti-virus software company
Search engine/the Internet
Family member or friend
Colleague or co-worker
Professional associations
A computer repair service
Someone from my company's IT department or service
My computer manufacturer/retailer
Other [anchor]
None of the above [anchor]

Just a few more questions for classification purposes.

26. What type of operating system does your personal computer have?

Windows (any version)
Mac (any version)
Linux (any version)
Other
Not sure

27. What is your employment status or profession?

Self employed
Employed full-time
Employed part-time
Retired
Homemaker
Unemployed
Student
Other

28. Are you of Hispanic descent? [Ask in US only]

Yes
No
Decline to answer

29. Please indicate your race: (Check ONE) [Ask in US only]

White
Black/African-American
Asian or Pacific Islander
Native American or Alaskan Native
Mixed racial background
Other
Decline to answer

French (Canada)

S1. Êtes-vous un homme ou une femme ?

Un homme
Une femme

S2. Quel âge avez-vous ?

18 à 24 ans
25 à 34 ans
35 à 44 ans
45 à 54 ans
55 à 64 ans
65 ans ou plus

S3. Quel est votre niveau d'éducation le plus élevé?

Études primaires ou une partie des études secondaires
Diplôme d'études secondaires
Diplôme d'études techniques/professionnelles/collégiales
Études collégiales ou universitaires (non diplômé)
Diplôme d'études universitaires, comme un baccalauréat
Diplôme d'études de deuxième ou troisième cycle, comme une maîtrise ou un doctorat

1. En ce qui concerne la sécurité sur Internet, y compris les pare-feu (« firewalls »), les pourriels (« spam »), les courriels indésirables et les virus informatiques, vous décririez-vous comme étant... ?

[REVERSE SCALE ON ½ SAMPLE]
Un(e) expert(e)
Très expérimenté(e)
Plutôt expérimenté(e)
Pas très expérimenté(e)
Pas du tout expérimenté(e)

2. Avez-vous uniquement une adresse courriel personnelle/privée, uniquement une adresse courriel d'affaires/fournie par votre employeur ou les deux ? [Single response]

Uniquement une adresse courriel personnelle/privée
Uniquement une adresse courriel d'affaires/fournie par votre employeur
Les deux

[ASK IF BOTH IN Q2]

3. S'agit-il d'adresses différentes ou de la même adresse ?

Adresses différentes
Même adresse

[ASK IF "BUSINESS/EMPLOYER-PROVIDED EMAIL ADDRESS ONLY" IN Q2 OR "SAME" IN Q3]

4. Est-ce que votre entreprise/employeur a un prestataire ou un service de TI ou une personne autre que vous qui gère la sécurité de votre adresse courriel d'affaires/fournie par votre employeur?

Oui [TERMINATE]
Non

5. En général, quelle importance accordez-vous à chacun des types suivants de courriels personnels qui vous sont envoyés ? Les considérez-vous comme étant…

ITEMS [Randomize]
Courriels d'amis et de membres de votre famille
Infolettres (« newsletters ») auxquelles vous êtes abonné(e)
Reçus ou détails d'envoi concernant des achats que vous avez effectués
Avis de factures à payer
Avis de votre banque ou d'une autre institution financière
Communications de marketing d'entreprises où vous avez effectué des achats ou comptez en faire
Autres courriels pour lesquels vous vous êtes inscrit(e) [anchor]

SCALE:
Extrêmement importants
Très importants
Plutôt importants
Pas très importants
Pas du tout importants

6. Lequel des énoncés suivants décrit le mieux l'ordinateur que vous utilisez le plus souvent pour votre courriel personnel ? [Single response]

Je mets moi-même à jour le logiciel antivirus quand cela est nécessaire
Une autre personne met à jour le logiciel antivirus quand cela est nécessaire
Personne ne met à jour le logiciel antivirus
Le logiciel antivirus se met à jour automatiquement
Il n'y a pas de logiciel antivirus sur cet ordinateur
Incertain(e)

[ASK IF “NOBODY UPDATES THE ANTI-VIRUS SOFTWARE” IN Q6]

7. Laquelle des raisons suivantes explique le mieux pourquoi votre logiciel antivirus n’est pas mis à jour ?

[Randomize]
Je suis incertain(e) de la façon de le mettre à jour
Il n’a pas besoin d’être mis à jour
Je n’ai jamais été appelé(e) à le mettre à jour
Je manque de temps/je remets à plus tard
Trop cher
Je n’ai jamais de virus
Aucune de ces réponses [anchor]

8. Personnellement, comment définissez-vous le « pourriel » ? Veuillez choisir tout ce qui s’applique.

[Randomize]
Courriel que je n’ai pas demandé
Courriel que j’ai déjà demandé, mais que je ne veux plus recevoir
Courriel pour de la pornographie, des médicaments, des augmentations de parties du corps, de casinos en ligne, etc.
Courriel contenant un virus ou courriel hameçon (« phishing »)
Courriel qui enfreint les règles anti-pourriel
Courriel dans mon répertoire de pourriels/courriels indésirables
Courriel de sources desquelles je ne peux pas me « désabonner »
Blagues et messages idiots qui me sont acheminés
Autrement [anchor]

9. Quelles mesures, s’il y a lieu, avez-vous prises pour garder votre boîte de courriels personnelle à l’abri des pourriels ? Veuillez choisir tout ce qui s’applique.

[Randomize]
Installé un filtre-courrier pour les pourriels ou les courriels indésirables
Ajouté à mon carnet d’adresses des expéditeurs que je reconnais
Déplacé des courriels que je ne voulais pas de ma boîte de réception à mon répertoire de pourriels
Utilisé une adresse courriel distincte lorsqu’il est possible que je reçoive des pourriels
Évité d’inscrire mon adresse courriel sur des sites Web
Évité de donner mon adresse courriel
Choisi une adresse courriel insolite difficile à deviner
Utilisé une adresse courriel distincte pour mes amis et ma famille
Autres [anchor]
Aucune de ces réponses [anchor]

10. Lorsque vous parcourez votre boîte de réception et décidez quels courriels sont des pourriels et lesquels sont pertinents, quels indicateurs utilisez-vous pour vous aider dans vos décisions ? Veuillez choisir tout ce qui s'applique.

[Randomize]
Le nom ou l'adresse de l'expéditeur
Le nom ou l'adresse du destinataire
La ligne « objet » ou « sujet »
L'heure de la journée/nuit à laquelle le message a été envoyé
Les icônes ou autres indicateurs visuels qui figurent à côté du message dans ma boîte de réception
Le contenu du courriel
Des fautes d'orthographe/une mauvaise grammaire
Un langage/une langue inhabituel(le)
Autres [anchor]
Je veux tous les courriels que je reçois [anchor]
Aucune de ces réponses [anchor]

11. Quand vous recevez un courriel que vous croyez être un pourriel, que faites-vous généralement ? Veuillez choisir tout ce qui s'applique.

[Randomize]
Je clique sur le bouton « Pourriel »
Je le déplace vers un répertoire « Indésirables »
Je le supprime sans l'identifier comme pourriel ou indésirable
Je ne l'ouvre pas
Je le lis sans ouvrir les pièces jointes ou cliquer sur les liens
Je le signale à mon fournisseur de service Internet ou de courriel
Je le signale à un service de signalement de pourriel/de pratiques abusives (p. ex., SpamCop, Abuse.net) ou à un organisme gouvernemental
Je change d'adresse courriel
J'utilise le lien « Désabonner »
Autre chose [anchor]
Aucune de ces réponses [anchor]

12. Avez-vous déjà fait l'une ou l'autre des choses suivantes ? Veuillez choisir tout ce qui s'applique.

[Randomize]
J'ai ouvert un courriel que je soupçonnais d'être un pourriel [anchor]
J'ai cliqué sur un lien dans un courriel que je soupçonnais d'être un pourriel
J'ai ouvert une pièce jointe dans un courriel que je soupçonnais d'être un pourriel
J'ai transféré un courriel que je soupçonnais d'être un pourriel
J'ai répondu à un courriel que je soupçonnais d'être un pourriel
Aucune de ces réponses [anchor]

[Ask if anything but “none of the above” in Q12]

13. Et pourquoi avez-vous fait cela ? Veuillez choisir tout ce qui s’applique.

[Randomize]
Le produit ou le service offert dans le courriel m’intéressait
Je voulais voir ce qui se passerait
Je l’ai fait par erreur
Je voulais me désabonner ou me plaindre à l’expéditeur
Je n’étais pas certain que c’était un pourriel
Autre raison [anchor]
Aucune de ces réponses [anchor]

14. Quand vous recevez un courriel que vous soupçonnez d’être frauduleux (p. ex., prétendant provenir d’une banque ou d’un marchand et demandant des renseignements personnels), que faites-vous généralement? Veuillez choisir tout ce qui s’applique.

[Randomize]
Je clique sur le bouton « Pourriel »
Je le déplace vers un répertoire « Indésirables »
Je le supprime sans l’identifier comme pourriel ou indésirable
Je ne l’ouvre pas
Je le lis sans ouvrir les pièces jointes ou cliquer sur les liens
Je le signale à mon fournisseur de service Internet ou de courriel
Je le signale à un service de signalement de pourriel/ de pratiques abusives (p. ex., SpamCop, Abuse.net) ou à un organisme gouvernemental
Je change d’adresse courriel
J’utilise le lien « Désabonner »
Je le signale à l’entreprise ou à l’institution concernée (p. ex., ma banque)
Je lance le logiciel antivirus
Je demande à un membre de ma famille ou à un ami ce qu’il faut faire
Autre chose [anchor]
Aucune de ces réponses [anchor]

15. Votre ordinateur a-t-il déjà été infecté par un virus?

Oui
Non

[ASK IF ‘YES’ IN Q15]

16. Quelle mesure, s’il y a lieu, avez-vous prise lorsque votre ordinateur a été infecté par un virus? Veuillez choisir tout ce qui s’applique.

[Randomize]
Signalé le virus à mon fournisseur de service Internet ou de courriel
Signalé le virus au fabricant de mon logiciel antivirus (p. ex., AVG, McAfee, Norton/Symantec)
Changé d’adresse courriel
Fait réparer l’ordinateur par un service de réparation à distance
Apporté mon ordinateur à un service de réparation
Réparé mon ordinateur moi-même
Fait réparer mon ordinateur par un ami ou un membre de ma famille
Lancé le logiciel antivirus
Autre chose [anchor]
Aucune de ces réponses [anchor]

17. Selon vous, à qui devrait incomber la plus grande part de responsabilité pour stopper la propagation des virus informatiques, des courriels frauduleux, des logiciels espions (« spyware ») et des pourriels? Veuillez choisir tout ce qui s'applique.

[Randomize]
Moi-même
Le Gouvernement/les organismes de protection des consommateurs
Les fournisseurs de service Internet et de service de courriel
Les détaillants de matériel informatique et de logiciels
Les associations professionnelles
Les grands fabricants de logiciels
Les fabricants d'ordinateurs
Les fabricants de logiciels antivirus
Les sites de réseautage social
Les groupes de défense des consommateurs
Autres [anchor]

18. Comment évalueriez-vous la performance de chacun des intervenants suivants pour ce qui est de stopper les virus informatiques, les courriels frauduleux, les logiciels espions et les pourriels ?

[Same order as Q17]
Moi-même
Le Gouvernement/les organismes de protection des consommateurs
Les fournisseurs de service Internet et de service de courriel
Les détaillants de matériel informatique et de logiciels
Les associations professionnelles
Les grands fabricants de logiciels
Les fabricants d'ordinateurs
Les fabricants de logiciels antivirus
Les sites de réseautage social
Les groupes de défense des consommateurs

Scale:
Très bonne
Plutôt bonne
Ni bonne ni mauvaise
Plutôt mauvaise
Très mauvaise

19. Dans quelle mesure connaissez-vous le terme « bot » ou « botnet » relatif à la propagation des pourriels et de virus informatiques ? [single response]

Il m'est très familier
Il m'est assez familier
J'en ai entendu parler, mais je n'en sais pas plus
Je n'en ai jamais entendu parler

20. Êtes-vous au courant de l'existence de virus malveillants qui peuvent contrôler votre ordinateur à votre insu et l'utiliser ensuite pour diffuser des pourriels ou voler vos renseignements personnels?

Oui
Non

21. Un « bot » ou « botnet » est un virus malveillant qui peut contrôler votre ordinateur à votre insu et l'utiliser ensuite pour diffuser des pourriels ou voler vos renseignements personnels. Dans quelle mesure est-il probable selon vous que votre ordinateur soit infecté par ce type de virus ?

[REVERSE SCALE ON ½ SAMPLE]
Extrêmement probable
Très probable
Plutôt probable
Pas très probable
Pas du tout probable
Incertain(e) [anchor]

22. Comment sauriez-vous si un « bot » ou un « botnet » se trouve sur votre ordinateur ? Veuillez choisir tout ce qui s'applique.

[Randomize]
Si mes amis me disaient qu'ils reçoivent des pourriels en provenance de mon adresse courriel
Si la société émettrice de ma carte de crédit ou ma banque m'avisait d'une activité suspecte dans mon compte
Si mon logiciel anti-virus m'en alertait
Si mon ordinateur ne fonctionnait pas normalement ou fonctionnait très lentement
Si des messages d'erreur inhabituels apparaissaient
Si je remarquais des fichiers corrompus
Si je remarquais un nouveau programme que je n'ai pas installé
Si un grand nombre de fenêtres intruses (« pop-ups ») s'ouvraient
Autrement [anchor]
Incertain(e) [anchor]

23. Lesquels des intervenants suivants tiendriez-vous responsable de réparer votre ordinateur s'il avait été infecté par un virus, un logiciel espion ou un bot/botnet ? Veuillez choisir tout ce qui s'applique.

[Same order as Q17]
Moi-même
Le Gouvernement/les organismes de protection des consommateurs
Les fournisseurs de service Internet et de service de courriel
Les détaillants de matériel informatique et de logiciels
Les associations professionnelles
Les grands fabricants de logiciels
Les fabricants d'ordinateurs
Les fabricants de logiciels antivirus
Les sites de réseautage social
Les groupes de défense des consommateurs
Autres [anchor]

24. Si vous découvriez que votre ordinateur a été infecté, comment régleriez-vous le problème ? Veuillez choisir tout ce qui s'applique.

[RANDOMIZE]
En faisant appel à mon fournisseur de service Internet ou de courriel qui le ferait à distance
En faisant appel à un service de réparation informatique qui le ferait à distance
En faisant appel au fabricant de mon logiciel antivirus qui le ferait à distance
En demandant à un membre de ma famille ou à un ami de le faire
En demandant à un professionnel de venir chez moi ou à mon bureau pour le faire
En apportant mon ordinateur à un service de réparation
Je réglerais le problème moi-même
Autrement [anchor]

25. Lesquelles des ressources suivantes utiliseriez-vous pour en savoir davantage sur la propagation des pourriels et des bots ou pour savoir comment mieux protéger votre ordinateur ? Veuillez choisir tout ce qui s'applique.

[RANDOMIZE]
Mon fournisseur de service Internet ou de courriel
Le fabricant de mon logiciel antivirus
Moteur de recherche/Internet
Membre de ma famille ou ami
Collègue de travail
Associations professionnelles
Service de réparation informatique
Quelqu'un du service de TI de mon entreprise
Le fabricant/détaillant de mon ordinateur
Autre [anchor]
Aucune de ces réponses [anchor]

Il ne reste que quelques questions qui serviront à des fins de classification.

26. Quel est le type de système d'exploitation de votre ordinateur personnel ?

Windows (n'importe quelle version)
Mac (n'importe quelle version)
Linux (n'importe quelle version)
Autre
Incertain(e)

27. Quelle est votre situation d'emploi ou professionnelle ?
Travailleur(se) autonome
Employé(e) à temps plein
Employé(e) à temps partiel
À la retraite
Au foyer
Sans emploi
Étudiant(e)
Autre

French (France)

S1. Êtes-vous un homme ou une femme ?

Un homme
Une femme

S2. Quel âge avez-vous ?

18 à 24 ans
25 à 34 ans
35 à 44 ans
45 à 54 ans
55 à 64 ans
65 ans ou plus

S3. Quel est votre plus haut niveau d'éducation ?

Aucun diplôme
Brevet des collèges
CAP/BEP
Baccalauréat ou équivalent
2 années d'université (DEUG)
3 années d'université (licence)
4 années d'université (maîtrise et au-delà)

1. En ce qui concerne la sécurité sur Internet, y compris les pare-feu (ou « firewalls »), les spams (ou « pourriels »), les e-mails (courriers électroniques) indésirables et les virus informatiques, vous décririez-vous comme étant... ?

[REVERSE SCALE ON ½ SAMPLE]
Un(e) expert(e)
Très expérimenté(e)
Plutôt expérimenté(e)
Pas très expérimenté(e)
Pas du tout expérimenté(e)

2. Avez-vous uniquement une adresse électronique (e-mail) personnelle/privée, uniquement une adresse électronique professionnelle/fournie par votre employeur ou les deux ? [Single response]

Uniquement une adresse électronique (e-mail) personnelle/privée
Uniquement une adresse électronique (e-mail) professionnelle/fournie par votre employeur
Les deux

[ASK IF BOTH IN Q2]

3. S'agit-il d'adresses différentes ou de la même adresse ?

Adresses différentes
Même adresse

[ASK IF "BUSINESS/EMPLOYER-PROVIDED EMAIL ADDRESS ONLY" IN Q2 OR "SAME" IN Q3]

4. Est-ce que votre entreprise/employeur a un prestataire ou un service informatique ou une personne autre que vous qui gère la sécurité de votre adresse électronique professionnelle/fournie par votre employeur ?

Oui [TERMINATE]
Non

5. En général, quelle importance accordez-vous à chacun des types suivants de courrier électronique personnel qui vous sont envoyés ? Les considérez-vous comme étant…

ITEMS [Randomize]
E-mails d'amis et de membres de votre famille
Lettres d'information (« newsletters ») auxquelles vous êtes abonné(e)
Reçus ou détails d'envoi concernant des achats que vous avez effectués
Avis de factures à payer
Avis de votre banque ou d'une autre institution financière
Offres commerciales d'entreprises où vous avez effectué des achats ou comptez en faire
Autres e-mails pour lesquels vous vous êtes inscrit(e) [anchor]

SCALE:
Extrêmement importants
Très importants
Plutôt importants
Pas très importants
Pas du tout importants

6. Lequel des énoncés suivants décrit le mieux l'ordinateur que vous utilisez le plus souvent pour votre courrier électronique personnel ? [Single response]

Je mets moi-même à jour le logiciel antivirus quand cela est nécessaire
Une autre personne met à jour le logiciel antivirus quand cela est nécessaire
Personne ne met à jour le logiciel antivirus
Le logiciel antivirus se met à jour automatiquement
Il n'y a pas de logiciel antivirus sur cet ordinateur
Incertain(e)

[ASK IF “NOBODY UPDATES THE ANTI-VIRUS SOFTWARE” IN Q6]

7. Laquelle des raisons suivantes explique le mieux pourquoi votre logiciel antivirus n’est pas mis à jour ?

[Randomize]
Je suis incertain(e) de la façon de le mettre à jour
Il n’a pas besoin d’être mis à jour
Je n’ai jamais été appelé(e) à le mettre à jour
Je manque de temps/je remets à plus tard
Trop cher
Je n’ai jamais de virus
Aucune de ces réponses [anchor]

8. Personnellement, comment définissez-vous le spam (ou « pourriel ») ? Veuillez choisir tout ce qui s’applique.

[Randomize]
Courrier électronique que je n’ai pas demandé
Courrier électronique que j’ai déjà demandé, mais que je ne veux plus recevoir
Courrier électronique pour de la pornographie, des médicaments, des augmentations de parties du corps, de casinos en ligne, etc.
Courrier électronique contenant un virus ou une escroquerie par « phishing » (ou « hameçonnage »)
Courrier électronique qui enfreint les règles anti-spam
Courrier électronique dans mon répertoire de spam ou de messages indésirables (« junk mail »)
Courrier électronique de sources desquelles je ne peux pas me « désabonner »
Blagues et messages idiots qui me sont acheminés
Autrement [anchor]

9. Quelles mesures, s’il y a lieu, avez-vous prises pour garder votre messagerie à l’abri des spams ? Veuillez choisir tout ce qui s’applique.

[Randomize]
Installé un filtre anti-spam ou anti-messages indésirables
Ajouté à mon carnet d’adresses des expéditeurs que je reconnais
Déplacé des messages que je ne voulais pas de ma boîte de réception à mon répertoire de spam
Utilisé une adresse e-mail distincte lorsqu’il est possible que je reçoive des spams
Évité d’inscrire mon adresse e-mail sur des sites Web
Évité de donner mon adresse e-mail
Choisi une adresse e-mail insolite difficile à deviner
Utilisé une adresse e-mail distincte pour mes amis et ma famille
Autres [anchor]
Aucune de ces réponses [anchor]

10. Lorsque vous parcourez votre boîte de réception et décidez quels e-mails sont des spams et lesquels sont pertinents, quels indicateurs utilisez-vous pour vous aider dans vos décisions ? Veuillez choisir tout ce qui s'applique.

[Randomize]
Le nom ou l'adresse de l'expéditeur
Le nom ou l'adresse du destinataire
La ligne « objet » ou « sujet »
L'heure de la journée/nuit à laquelle le message a été envoyé
Les icônes ou autres indicateurs visuels qui figurent à côté du message dans ma boîte de réception
Le contenu de l'e-mail
Des fautes d'orthographe/une mauvaise grammaire
Un langage/une langue inhabituel(le)
Autres [anchor]
Je veux tous les e-mails que je reçois [anchor]
Aucune de ces réponses [anchor]

11. Quand vous recevez un e-mail que vous croyez être un spam, que faites-vous généralement ? Veuillez choisir tout ce qui s'applique.

[Randomize]
Je clique sur le bouton « Spam »
Je le déplace vers un répertoire « Indésirables »
Je le supprime sans l'identifier comme spam ou indésirable
Je ne l'ouvre pas
Je le lis sans ouvrir les pièces jointes ou cliquer sur les liens
Je le signale à mon prestataire de service Internet ou d'e-mail
Je le signale à un service de signalement de spam/de pratiques abusives (ex. SpamCop, Abuse.net) ou à un organisme gouvernemental
Je change d'adresse e-mail
J'utilise le lien « Désabonner »
Autre chose [anchor]
Aucune de ces réponses [anchor]

12. Avez-vous déjà fait l'une ou l'autre des choses suivantes ? Veuillez choisir tout ce qui s'applique.

[Randomize]
J'ai ouvert un e-mail que je soupçonnais d'être un spam [anchor]
J'ai cliqué sur un lien dans un e-mail que je soupçonnais d'être un spam
J'ai ouvert une pièce jointe dans un e-mail que je soupçonnais d'être un spam
J'ai fait suivre un spam que je soupçonnais d'être un spam
J'ai répondu à un e-mail que je soupçonnais d'être un spam
Aucune de ces réponses [anchor]

[Ask if anything but “none of the above” in Q12]

13. Et pourquoi avez-vous fait cela ? Veuillez choisir tout ce qui s’applique.

[Randomize]
Le produit ou le service offert dans l’e-mail m’intéressait
Je voulais voir ce qui se passerait
Je l’ai fait par erreur
Je voulais me désabonner ou me plaindre à l’expéditeur
Je n’étais pas certain que c’était un spam
Autre raison [anchor]
Aucune de ces réponses [anchor]

14. Quand vous recevez un e-mail que vous soupçonnez d’être frauduleux (par exemple, prétendant provenir d’une banque ou d’un commerce et demandant des renseignements personnels), que faites-vous généralement? Veuillez choisir tout ce qui s’applique.

[Randomize]
Je clique sur le bouton « Spam »
Je le déplace vers un répertoire « Indésirables »
Je le supprime sans l’identifier comme spam ou indésirable
Je ne l’ouvre pas
Je le lis sans ouvrir les pièces jointes ou cliquer sur les liens
Je le signale à mon prestataire de service Internet ou d’e-mail
Je le signale à un service de signalement de spam/ de pratiques abusives (ex. SpamCop, Abuse.net) ou à un organisme gouvernemental
Je change d’adresse e-mail
J’utilise le lien « Désabonner »
Je le signale à l’entreprise ou à l’institution concernée (ex. ma banque)
Je lance le logiciel antivirus
Je demande à un membre de ma famille ou à un ami ce qu’il faut faire
Autre chose [anchor]
Aucune de ces réponses [anchor]

15. Votre ordinateur a-t-il déjà été infecté par un virus?

Oui
Non

[ASK IF ‘YES’ IN Q15]

16. Quelle mesure, s’il y a lieu, avez-vous prise lorsque votre ordinateur a été infecté par un virus? Veuillez choisir tout ce qui s’applique.

[Randomize]
Signalé le virus à mon prestataire de service Internet ou d’e-mail
Signalé le virus au fabricant de mon logiciel antivirus (ex. AVG, McAfee, Norton/Symantec)
Changé d’adresse e-mail
Fait réparer l’ordinateur par un service de réparation à distance
Apporté mon ordinateur à un service de réparation
Réparé mon ordinateur moi-même
Fait réparer mon ordinateur par un ami ou un membre de ma famille
Lancé le logiciel antivirus
Autre chose [anchor]
Aucune de ces réponses [anchor]

17. Selon vous, à qui devrait incomber la plus grande part de responsabilité pour stopper la propagation des virus informatiques, des e-mails frauduleux, des logiciels espions (« spyware ») et des spams ? Veuillez choisir tout ce qui s'applique.

[Randomize]
Moi-même
L'Etat/les organismes de protection des consommateurs
Les prestataires de service Internet et d'e-mail
Les détaillants de matériel informatique et de logiciels
Les associations professionnelles
Les grands fabricants de logiciels
Les fabricants d'ordinateurs
Les fabricants de logiciels antivirus
Les réseaux sociaux en ligne
Les associations de consommateurs
Autres [anchor]

18. Comment évalueriez-vous la performance de chacun des intervenants suivants pour ce qui est de stopper les virus informatiques, les e-mails frauduleux, les logiciels espions et les spams ?

[Same order as Q17]
Moi-même
L'Etat/les organismes de protection des consommateurs
Les prestataires de service Internet et d'e-mail
Les détaillants de matériel informatique et de logiciels
Les associations professionnelles
Les grands fabricants de logiciels
Les fabricants d'ordinateurs
Les fabricants de logiciels antivirus
Les réseaux sociaux en ligne
Les associations de consommateurs

Scale:
Très bonne
Plutôt bonne
Ni bonne ni mauvaise
Plutôt mauvaise
Très mauvaise

19. Dans quelle mesure connaissez-vous le terme « bot » ou « botnet » relatif à la propagation de spams et de virus informatiques ? [single response]

Il m'est très familier
Il m'est assez familier
J'en ai entendu parler, mais je n'en sais pas plus
Je n'en ai jamais entendu parler

20. Êtes-vous au courant de l'existence de virus malveillants qui peuvent contrôler votre ordinateur à votre insu et l'utiliser ensuite pour diffuser des spams ou voler vos renseignements personnels ?

Oui
Non

21. Un « bot » ou « botnet » est un virus malveillant qui peut contrôler votre ordinateur à votre insu et l'utiliser ensuite pour diffuser des spams ou voler vos renseignements personnels. Dans quelle mesure est-il probable selon vous que votre ordinateur soit infecté par ce type de virus ?

[REVERSE SCALE ON ½ SAMPLE]
Extrêmement probable
Très probable
Plutôt probable
Pas très probable
Pas du tout probable
Incertain(e) [anchor]

22. Comment sauriez-vous si un « bot » ou un « botnet » se trouve sur votre ordinateur ? Veuillez choisir tout ce qui s'applique.

[Randomize]
Si mes amis me disaient qu'ils reçoivent des spams en provenance de mon adresse e-mail
Si la société émettrice de ma carte de crédit ou ma banque m'avisait d'une activité suspecte dans mon compte
Si mon logiciel anti-virus m'en alertait
Si mon ordinateur ne fonctionnait pas normalement ou fonctionnait très lentement
Si des messages d'erreur inhabituels apparaissaient
Si je remarquais des fichiers corrompus
Si je remarquais un nouveau programme que je n'ai pas installé
Si un grand nombre de fenêtres intruses (« pop-ups ») s'ouvraient
Autrement [anchor]
Incertain(e) [anchor]

23. Lesquels des intervenants suivants tiendriez-vous responsable de réparer votre ordinateur s'il avait été infecté par un virus, un logiciel espion ou un bot/botnet ? Veuillez choisir tout ce qui s'applique.

[Same order as Q17]
Moi-même
L'Etat/les organismes de protection des consommateurs
Les prestataires de service Internet et d'e-mail
Les détaillants de matériel informatique et de logiciels
Les associations professionnelles
Les grands fabricants de logiciels
Les fabricants d'ordinateurs
Les fabricants de logiciels antivirus
Les réseaux sociaux en ligne
Les associations de consommateurs
Autres [anchor]

24. Si vous découvriez que votre ordinateur a été infecté, comment régleriez-vous le problème ? Veuillez choisir tout ce qui s'applique.

[RANDOMIZE]
En faisant appel à mon prestataire de service Internet ou d'e-mail qui le ferait à distance
En faisant appel à un service de réparation informatique qui le ferait à distance
En faisant appel au fabricant de mon logiciel antivirus qui le ferait à distance
En demandant à un membre de ma famille ou à un ami de le faire
En demandant à un professionnel de venir chez moi ou à mon bureau pour le faire
En apportant mon ordinateur à un service de réparation
Je réglerais le problème moi-même
Autrement [anchor]

25. Lesquelles des ressources suivantes utiliseriez-vous pour en savoir davantage sur la propagation des spams et des bots ou pour savoir comment mieux protéger votre ordinateur ? Veuillez choisir tout ce qui s'applique.

[RANDOMIZE]
Mon prestataire de service Internet ou d'e-mail
Le fabricant de mon logiciel antivirus
Moteur de recherche/Internet
Membre de ma famille ou ami
Collègue de travail
Associations professionnelles
Service de réparation informatique
Quelqu'un du service informatique de mon entreprise
Le fabricant ou le revendeur de mon ordinateur
Autre [anchor]
Aucune de ces réponses [anchor]

Il ne reste que quelques questions qui serviront à des fins de classification.

26. Quel est le type de système d'exploitation de votre ordinateur personnel ?

Windows (n'importe quelle version)
Mac (n'importe quelle version)
Linux (n'importe quelle version)
Autre
Incertain(e)

27. Quelle est votre situation d'emploi ou professionnelle ?

Travailleur(se) indépendant(e)/à mon compte
Employé(e) à temps plein
Employé(e) à temps partiel
Retraité(e)
Au foyer
Sans emploi
Étudiant(e)
Autre

German (Germany)

S1. Bitte geben Sie Ihr Geschlecht an:

Männlich
Weiblich

S2. Wie alt sind Sie?

18 bis 24
25 bis 34
35 bis 44
45 bis 54
55 bis 64
65 oder älter

S3. Welchen höchsten Schulabschluss haben Sie bisher erreicht?

Hauptschule (9 Jahre) ohne abgeschlossene Berufsausbildung
Hauptschule (9 Jahre] mit abgeschlossener Berufsausbildung
Realschule (10 Jahre) ohne Hochschulreife
Hochschulreife (12-13 Jahre)
Hochschulausbildung (z. B. Universitäts- oder Fachhochschulstudium)

1. Wie würden Sie sich selbst im Hinblick auf Ihre Erfahrung mit Sicherheit im Internet beschreiben, u. a. in Bezug auf Firewalls, Spam, Junk-Mail und Computerviren?

[REVERSE SCALE ON ½ SAMPLE]
Experte
Viel Erfahrung
Etwas Erfahrung
Kaum Erfahrung
Keine Erfahrung

2. Haben Sie nur eine private E-Mail-Adresse, nur eine geschäftliche/vom Arbeitgeber bereitgestellte E-Mail-Adresse oder beides? [Single response]

Nur eine private E-Mail-Adresse
Nur eine geschäftliche/vom Arbeitgeber bereitgestellte E-Mail-Adresse
Beides

[ASK IF BOTH IN Q2]
3. Sind diese E-Mail-Adressen unterschiedlich oder gleich?

Unterschiedlich
Gleich

[ASK IF “BUSINESS/EMPLOYER-PROVIDED EMAIL ADDRESS ONLY” IN Q2 OR “SAME” IN Q3]

4. Verfügt Ihr Unternehmen/Ihr Arbeitgeber über einen IT-Service, eine Abteilung oder einen Mitarbeiter (abgesehen von Ihnen selbst), der die Sicherheit der geschäftlichen/vom Arbeitgeber bereitgestellten E-Mail-Adresse verwaltet?

Ja [TERMINATE]
Nein

5. Für wie wichtig halten Sie die folgenden Arten privater E-Mail, die Sie erhalten, insgesamt?

ITEMS [Randomize]
E-Mail von Freunden und Angehörigen
Abonnierte Newsletter
Quittungen oder Lieferdaten von getätigten Einkäufen
Benachrichtigungen über fällige Rechnungen
Benachrichtigungen Ihrer Bank oder anderer Finanzinstitute
Marketing und Angebote von Unternehmen, deren Produkte Sie gekauft haben bzw. zu kaufen planen
Andere E-Mail, für die Sie sich angemeldet haben [anchor]

SCALE:
Äußerst wichtig
Sehr wichtig
Eher wichtig
Nicht sehr wichtig
Völlig unwichtig

6. Welche der folgenden Aussagen trifft am stärksten auf den Computer zu, den Sie am häufigsten für Ihre private E-Mail verwenden? [Single response]

Ich aktualisiere die Antivirensoftware persönlich nach Bedarf
Jemand anderes aktualisiert die Antivirensoftware nach Bedarf
Niemand aktualisiert die Antivirensoftware
Die Antivirensoftware aktualisiert sich automatisch
Es ist keine Antivirensoftware auf dem Computer installiert
Nicht sicher

[ASK IF “NOBODY UPDATES THE ANTI-VIRUS SOFTWARE” IN Q6]

7. Welcher der folgenden Gründe beschreibt am besten, weshalb Ihre Antivirensoftware nicht aktualisiert wird?

[Randomize]
Ich weiß nicht genau, wie ich vorgehen muss
Sie muss nicht aktualisiert werden
Ich wurde noch nie aufgefordert, sie zu aktualisieren
Ich habe nicht genügend Zeit/habe die Aufgabe immer verschoben
Zu teuer
Ich bekomme nie Viren
Keiner dieser Gründe [anchor]

8. Wie definieren Sie persönlich Spam? Bitte wählen Sie alle zutreffenden Antworten aus.

[Randomize]
Nicht angeforderte E-Mail
E-Mail, die ich angefordert habe, jetzt aber nicht mehr erhalten möchte
E-Mail, die Pornografie, Medikamente, Körperteilvergrößerung, Online-Casinos usw. bewirbt
E-Mail, die Viren oder Phishing enthält
E-Mail, die gegen Anti-Spam-Vorschriften verstößt
E-Mail in meinem Spam- oder Junk-Mail-Ordner
E-Mail von Quellen, die kein Abmelden erlauben
Witze und alberne Nachrichten, die an mich weitergeleitet werden
Sonstige [anchor]

9. Was haben Sie ggf. unternommen, um Ihren E-Mail-Eingang frei von Spam zu halten? Bitte wählen Sie alle zutreffenden Antworten aus.

[Randomize]
Spam- oder Junk-Mail-Filter installiert
Bekannte Absender zu meinem Adressbuch hinzugefügt
Unerwünschte E-Mail von meinem Posteingang in den Junk-Mail-/Spam-Ordner verschoben
Getrennte E-Mail-Adresse verwendet, wo Spam hätte auftreten können
Meine E-Mail-Adresse nicht auf Websites veröffentlicht
Meine E-Mail-Adresse nicht weitergegeben
Eine ungewöhnliche E-Mail-Adresse eingerichtet, die schwer zu erraten ist
Verwende eine getrennte E-Mail-Adresse für Freunde und Angehörige
Sonstige [anchor]
Keine der Obigen [anchor]

10. Auf welche Indikatoren verlassen Sie sich beim Durchgehen Ihres Posteingangs, um zu entscheiden, was Spam und was legitime E-Mail darstellt? Bitte wählen Sie alle zutreffenden Antworten aus.

[Randomize]
Name oder Adresse des Absenders
Name oder Adresse des Empfängers
Betreffzeile
Uhrzeit des Verschickens
Die Symbole oder anderen grafischen Anzeigen in meinem Posteingang neben der Nachricht
Den Inhalt der E-Mail
Rechtschreib- und Grammatikfehler
Ungewöhnliche Sprache/Wortwahl
Sonstige [anchor]
Sämtliche E-Mail, die ich erhalte, ist erwünscht [anchor]
Keine der Obigen [anchor]

11. Was tun Sie üblicherweise, wenn Sie E-Mail erhalten, die Sie für Spam halten? Bitte wählen Sie alle zutreffenden Antworten aus.

[Randomize]
Ich wähle die Schaltfläche, mit der die E-Mail als Spam eingeordnet wird
Ich verschiebe die E-Mail in den Ordner für Junk-Mail
Ich lösche die E-Mail, ohne sie als Spam oder Junk-Mail zu markieren
Ich öffne die E-Mail nicht
Ich lese die E-Mail, ohne Anhänge zu öffnen oder auf Links zu klicken
Ich melde die E-Mail meinem Internet- bzw. E-Mail-Anbieter
Ich melde die E-Mail einem externen Spam-/E-Mail-Missbrauchsdienst, wie z. B. SpamCop oder Abuse.net oder einer Behörde
Ich ändere meine E-Mail-Adresse
Ich verwende den Link zum Abmelden
Sonstige [anchor]
Keine der Obigen [anchor]

12. Haben Sie je eines der folgenden Dinge getan? Bitte wählen Sie alle zutreffenden Antworten aus.

[Randomize]
Eine E-Mail trotz Spamverdacht geöffnet [anchor]
Trotz Spamverdacht auf einen Link in einer E-Mail geklickt
Trotz Spamverdacht einen E-Mail-Anhang geöffnet
Eine E-Mail trotz Spamverdacht weitergeleitet
Eine E-Mail trotz Spamverdacht beantwortet
Keine der Obigen [anchor]

[Ask if anything but “none of the above” in Q12]
13. Weshalb haben Sie so gehandelt?
(Bitte wählen Sie alle zutreffenden Antworten aus.)

[Randomize]
Ich war am angebotenen Produkt bzw. Service interessiert
Ich wollte schauen, was passiert
Ich habe das versehentlich getan
Ich wollte mich abmelden bzw. mich beim Absender beschweren
Ich war mir nicht sicher, dass es sich um Spam handelte
Sonstige [anchor]
Keine der Obigen [anchor]

14. Was tun Sie in der Regel, wenn Sie E-Mail erhalten, die Sie für betrügerisch halten (z. B. E-Mail, die vorgeblich von einer Bank oder einem Händler stammt und in der Sie um persönliche Informationen gebeten werden)? Bitte wählen Sie alle zutreffenden Antworten aus.

[Randomize]
Ich wähle die Schaltfläche, mit der die E-Mail als Spam eingeordnet wird
Ich verschiebe die E-Mail in den Ordner für Junk-Mail
Ich lösche die E-Mail, ohne sie als Spam oder Junk-Mail zu markieren
Ich öffne die E-Mail nicht
Ich lese die E-Mail, ohne Anhänge zu öffnen oder auf Links zu klicken
Ich melde die E-Mail meinem Internet- bzw. E-Mail-Anbieter
Ich melde die E-Mail einem externen Spam-/E-Mail-Missbrauchsdienst, wie z. B. SpamCop oder Abuse.net oder einer Behörde
Ich ändere meine E-Mail-Adresse
Ich verwende den Link zum Abmelden
Ich melde die Angelegenheit einem legitimen Unternehmen/einer legitimen Institution (z. B. meiner Bank)
Ich führe mein Antivirenprogramm aus
Ich frage Angehörige oder Freunde, was ich tun soll
Sonstige [anchor]
Keine der Obigen [anchor]

15. Wurde Ihr Computer je von einem Virus befallen?

Ja
Nein

[ASK IF 'YES' IN Q15]
16. Was haben Sie unternommen, als Ihr Computer von einem Virus befallen war? Bitte wählen Sie alle zutreffenden Antworten aus.

[Randomize]
Ich habe den Virus meinem Internet- bzw. E-Mail-Anbieter gemeldet
Ich habe den Virus dem Anbieter meines Antivirenprogramms (z. B. AVG, McAfee, Norton/Symantec, usw.) gemeldet
Ich habe meine E-Mail-Adresse geändert
Ich ließ das Problem fern durch einen Computerreparaturdienst beheben
Ich habe meinen Computer zu einem Computerreparaturdienst gebracht
Ich habe den Computer selbst repariert
Ich ließ den Computer von einem Freund oder Angehörigen reparieren
Ich habe mein Antivirenprogramm ausgeführt
Sonstige [anchor]
Keine der Obigen [anchor]

17. Wer sollte Ihrer Ansicht nach am meisten Verantwortung dafür übernehmen, die Verbreitung von Computerviren, betrügerischer E-Mail, Spyware und Spam zu verhindern? Bitte wählen Sie alle zutreffenden Antworten aus.

[Randomize]
Ich selbst
Regierung/Verbraucherschutzbehörden
Internet- und E-Mail-Anbieter
Computer- und Softwarehändler
Berufsverbände
Führende Computersoftwareanbieter
Computerhersteller
Anbieter von Antivirensoftware
Websites für soziale Netzwerke
Verbraucherschutzgruppen
Sonstige [anchor]

18. Wie beurteilen Sie die Leistung der Folgenden beim Aufhalten der Verbreitung von Computerviren, betrügerischer E-Mail, Spyware und Spam?

[Same order as Q17]
Ich selbst
Regierung/Verbraucherschutzbehörden
Internet- und E-Mail-Anbieter
Computer- und Softwarehändler
Berufsverbände
Führende Computersoftwareanbieter
Computerhersteller
Anbieter von Antivirensoftware
Websites für soziale Netzwerke
Verbraucherschutzgruppen

Scale:
Sehr gut
Ziemlich gut
Weder gut noch schlecht
Ziemlich schlecht
Sehr schlecht

19. Wie vertraut ist Ihnen der Begriff „Bot“ bzw. „Botnet“ im Hinblick auf Spam und Computerviren? [single response]

Sehr vertraut
Eher vertraut
Habe davon gehört, weiß jedoch nichts darüber
Nie davon gehört

20. Sind Sie sich der Tatsache bewusst, dass es bösartige Viren gibt, die Ihren Computer ohne Ihr Wissen kontrollieren und diesen anschließend für die Verbreitung von Spam bzw. für den Diebstahl Ihrer persönlichen Daten verwenden können?

Ja
Nein

21. Ein „Bot“ bzw. „Botnet“ ist ein bösartiger Virus, der Ihren Computer ohne Ihr Wissen kontrollieren und diesen anschließend für die Verbreitung von Spam bzw. für den Diebstahl Ihrer persönlichen Daten

verwenden kann. Für wie wahrscheinlich halten Sie es, dass Ihr Computer mit einem derartigen Virus infiziert werden könnte?

[REVERSE SCALE ON ½ SAMPLE]
Äußerst wahrscheinlich
Sehr wahrscheinlich
Eher wahrscheinlich
Eher unwahrscheinlich
Sehr unwahrscheinlich
Nicht sicher [anchor]

22. Woher wüssten Sie, ob Ihr Computer mit einem „Bot“ oder „Botnet“ infiziert ist? Bitte wählen Sie alle zutreffenden Antworten aus.

[Randomize]
Wenn mir meine Freunde berichten würden, dass sie Spam von meiner E-Mail-Adresse erhalten
Wenn mein Kreditkartenunternehmen bzw. meine Bank mich über verdächtige Transaktionen informieren würde
Wenn meine Antivirensoftware mich darauf hinweisen würde
Wenn mein Computer nicht normal funktionieren oder besonders langsam laufen würde
Wenn ungewöhnliche Fehlermeldungen auftreten würden
Wenn ich beschädigte Dateien bemerken würde
Wenn ich ein neues Programm bemerken würde, das ich nicht installiert habe
Wenn viele Popup-Fenster angezeigt würden
Sonstige [anchor]
Nicht sicher [anchor]

23. Welche der Folgenden würden Sie für Viren, Spyware oder Bots/Botnets auf Ihrem Computer verantwortlich machen? Bitte wählen Sie alle zutreffenden Antworten aus.

[Same order as Q17]
Mich selbst
Regierung/Verbraucherschutzbehörden
Internet- oder E-Mail-Anbieter
Computer- oder Softwarehändler
Berufsverbände
Computersoftwareanbieter
Computerhersteller
Anbieter von Antivirensoftware
Websites für soziale Netzwerke
Verbraucherschutzgruppen
Sonstige [anchor]

24. Wie würden Sie Ihren Computer reparieren lassen, wenn Sie eine Infektion feststellen würden? Bitte wählen Sie alle zutreffenden Antworten aus.

[RANDOMIZE]
Fern durch meinen Internet- bzw. E-Mail-Anbieter
Fern durch einen Computerreparaturdienst
Fern durch den Anbieter meiner Antivirensoftware
Durch einen Angehörigen oder Freund
Durch Hinzuziehen eines Fachmanns, der den Computer bei mir zuhause/im Büro repariert
Indem ich den Computer zu einem Reparaturdienst bringe
Ich würde ihn selbst reparieren
Sonstige [anchor]

25. Welche der folgenden Ressourcen würden Sie verwenden, um mehr über Spam und Bots bzw. über bessere Schutzmöglichkeiten für Ihren Computer zu erfahren? Bitte wählen Sie alle zutreffenden Antworten aus.

[RANDOMIZE]
Meinen Internet- bzw. E-Mail-Anbieter
Meinen Anbieter von Antivirensoftware
Suchmaschinen/Internet
Angehörige oder Freunde
Kollegen oder Mitarbeiter
Berufsverbände
Computerreparaturdienst
Mitarbeiter der IT-Abteilung/des IT-Service meines Unternehmens
Meinen Computerhersteller/-händler
Sonstige [anchor]
Keine der Obigen [anchor]

Abschließend möchten wir Ihnen noch einige Fragen zu Klassifizierungszwecken stellen.

26. Welches Betriebssystem verwenden Sie auf Ihrem PC?

Windows (jegliche Version)
Mac OS (jegliche Version)
Linux (jegliche Version)
Sonstiges
Nicht sicher

27. Bitte geben Sie Ihren Beschäftigungsstatus bzw. Ihren Beruf an.

Selbstständig
Vollzeitbeschäftigt
Teilzeitbeschäftigt
Im Ruhestand
Hausfrau/-mann
Arbeitslos
Student/Schüler
Sonstige

Spanish (Spain)

S1. ¿Cuál es su sexo?

Hombre
Mujer

S2. ¿Cuántos años tiene?

18 a 24
25 a 34
35 a 44
45 a 54
55 a 64
65 o más

S3. ¿Cuál es el nivel más alto de educación formal que usted ha terminado?

Nada/Primaria no terminada
Primaria terminada
Secundaria terminada
Secundaria terminada o formación profesional
Nivel medio de universidad
Nivel superior de universidad
Posgrado/Doctorado

1. ¿Cómo se describiría a sí mismo con respecto a su experiencia con la seguridad en Internet, incluidos cortafuegos (firewalls), spam, correo basura y virus informáticos?

[REVERSE SCALE ON ½ SAMPLE]
Un experto
Con mucha experiencia
Con algo de experiencia
Con poca experiencia
Sin ninguna experiencia

2. ¿Dispone únicamente de una dirección de correo electrónico (e-mail) personal/de casa, únicamente de una dirección de correo electrónico de trabajo/proporcionada por su empresa o de ambas? [Single response]

Únicamente una dirección de correo electrónico (e-mail) personal/de casa
Únicamente una dirección de correo electrónico (e-mail) de trabajo/proporcionada por la empresa
Ambas

[ASK IF BOTH IN Q2]
3. ¿Se trata de direcciones diferentes o se trata de la misma?

Diferentes
La misma

[ASK IF “BUSINESS/EMPLOYER-PROVIDED EMAIL ADDRESS ONLY” IN Q2 OR “SAME” IN Q3]

4. ¿Cuenta su negocio/empresa con una persona, departamento o servicio de TI distintos a usted que gestionen la seguridad de su dirección de correo electrónico de trabajo/proporcionada por su empresa?

Sí [TERMINATE]
No

5. En general, ¿qué importancia concede a cada uno de los siguientes tipos de mensajes personales de correo electrónico que recibe?

ITEMS [Randomize]
Mensajes de amigos y familiares
Boletines a los que se ha suscrito
Recibos o información de envío de compras que ha realizado
Notificaciones de facturas pendientes de pago
Notificaciones de su banco o de otras instituciones financieras
Marketing de empresas en las que ha realizado una compra o a las cuales piensa hacer una compra
Otro correo electrónico en el que esté registrado [anchor]

SCALE:
Extremadamente importantes
Muy importantes
Algo importantes
No son muy importantes
Nada importantes

6. ¿Cuál de las siguientes opciones describe mejor el ordenador que utiliza con más frecuencia para su correo personal? [Single response]

Actualizo personalmente el software antivirus cuando es necesario hacerlo
Otra persona actualiza el software antivirus cuando es necesario hacerlo
Nadie actualiza el software antivirus
El software antivirus se actualiza automáticamente
No hay software antivirus en este ordenador
No estoy seguro

[ASK IF "NOBODY UPDATES THE ANTI-VIRUS SOFTWARE" IN Q6]

7. ¿Cuál de las siguientes razones describe mejor el motivo por el que no se actualiza su software antivirus?

[Randomize]
No estoy seguro sobre cómo actualizarlo
No es necesario actualizarlo
Nunca se me ha solicitado que lo actualice
No tengo tiempo/lo he pospuesto para hacerlo más adelante
Es demasiado caro
No he tenido nunca un virus
Ninguna de las anteriores [anchor]

8. ¿Cómo define personalmente el spam? Seleccione todas las opciones que correspondan.

[Randomize]
Correo electrónico que no he solicitado
Correo electrónico que he solicitado una vez pero que ya no deseo recibir
Correo electrónico de porno, pastillas, aumento de partes del cuerpo, casinos en línea, etc.
Correo electrónico que contiene un virus o un plan de *phishing*
Correo electrónico que infringe las leyes antispam
Correo electrónico en mi carpeta de spam o de correo basura
Correo electrónico procedente de fuentes de las cuales no puedo cancelar la suscripción
Chistes y mensajes tontos que me reenvían
Otros [anchor]

9. ¿Qué medidas ha tomado, si es que ha tomado alguna, para mantener la bandeja de entrada de correo electrónico personal libre de spam? Seleccione todas las opciones que correspondan.

[Randomize]
He instalado un filtro de spam o de correo basura
He añadido remitentes que reconozco a mi libreta de direcciones
He pasado los mensajes que no quería de mi bandeja de entrada a la carpeta de correo basura o spam
He utilizado una dirección de correo electrónico diferente cuando existe la posibilidad de recibir spam
He evitado incluir mi dirección de correo electrónico en páginas de Internet
He evitado proporcionar mi dirección de correo electrónico
He creado una dirección de correo electrónico fuera de lo común que es difícil de adivinar
He utilizado una dirección de correo electrónico diferente para amigos y familiares
Otra [anchor]
Ninguna de las anteriores [anchor]

10. Cuando repasa su buzón de correo electrónico y decide qué mensajes son spam y cuáles son legítimos, ¿en qué indicadores se basa para tomar la decisión? Seleccione todas las opciones que correspondan

[Randomize]
La dirección o el nombre del remitente
La dirección o el nombre del receptor
El texto del asunto
La hora del día/noche en que se envió
Los iconos u otros indicadores visuales que aparecen en mi bandeja de entrada junto al mensaje
El contenido del correo electrónico
Faltas de ortografía/gramática incorrecta
Lenguaje inusual
Otra [anchor]
Quiero todo el correo electrónico que recibo [anchor]
Ninguna de las anteriores [anchor]

11. Cuando recibe correo electrónico que cree que es spam, ¿qué es lo que suele hacer? Seleccione todas las opciones que correspondan.

[Randomize]
Darle al botón “Esto es spam”
Pasarlo a una carpeta de “correo basura”
Borrarlo sin marcarlo como spam o correo basura
No lo abro
Lo leo sin abrir ningún archivo adjunto ni pinchar en ningún enlace
Informo de ello a mi proveedor de servicio de Internet o a mi proveedor de servicio de correo electrónico
Informo de ello a un servicio independiente de notificación de spam o abuso de correo electrónico (p. ej., SpamCop, Abuse.net) o a una agencia gubernamental
Cambio mi dirección de correo electrónico
Utilizo el enlace “Cancelar suscripción”
Otra [anchor]
Ninguna de las anteriores [anchor]

12. ¿Ha hecho alguna vez alguna de las siguientes cosas? Seleccione todas las opciones que correspondan.

[Randomize]
He abierto un correo electrónico que sospechaba que era spam [anchor]
He pinchado en un enlace en un correo electrónico que sospechaba que era spam
He abierto un archivo adjunto en un correo electrónico que sospechaba que era spam
He reenviado un correo electrónico que sospechaba que era spam
He contestado a un correo electrónico que sospechaba que era spam
Ninguna de las anteriores [anchor]

[Ask if anything but “none of the above” in Q12]

13. ¿Y por qué ha hecho esto?
(Múltiples respuestas)

[Randomize]
Estaba interesado en el producto o servicio ofrecidos en el mensaje
Quería ver qué pasaba
Lo hice por error
Quería cancelar la suscripción o quejarme al remitente
No estaba seguro de que se tratase de spam
Otra [anchor]
Ninguna de las anteriores [anchor]

14. Cuando recibe correo que sospecha que es fraudulento (p. ej., aparenta proceder de un banco o un comerciante y le solicita datos personales), ¿qué suele hacer? Seleccione todas las opciones que correspondan.

[Randomize]
Darle al botón “Esto es spam”
Pasarlo a una carpeta de “correo basura”
Borrarlo sin marcarlo como spam o correo basura
No lo abro
Lo leo sin abrir ningún archivo adjunto ni pinchar en ningún enlace
Informo de ello a mi proveedor de servicio de Internet o a mi proveedor de servicio de correo electrónico
Informo de ello a un servicio independiente de notificación de spam o abuso de correo electrónico (p. ej., SpamCop, Abuse.net) o a una agencia gubernamental
Cambio mi dirección de correo electrónico
Utilizo el enlace “Cancelar suscripción”
Informo de ello a la institución o empresa legítima (p. ej., mi banco)
Ejecuto mi software antivirus
Pregunto a un familiar o amigo qué tengo que hacer
Otra [anchor]
Ninguna de las anteriores [anchor]

15. ¿Se ha visto afectado en alguna ocasión su ordenador por un virus?

Sí
No

[ASK IF 'YES' IN Q15]

16. ¿Qué medida tomó, si tomó alguna, cuando se infectó su ordenador con un virus? Seleccione todas las opciones que correspondan.

[Randomize]
Informé de ello a mi proveedor de servicio de Internet o a mi proveedor de servicio de correo electrónico
Informé sobre el virus a la empresa de mi software antivirus (p. ej., AVG, McAfee, Norton/Symantec, etc.)
Cambié mi dirección de correo electrónico
Lo hice reparar remotamente por un servicio de reparación de ordenadores
Llevé mi ordenador a un servicio de reparación de ordenadores
Reparé yo mismo el ordenador
Un amigo o familiar reparó mi ordenador
Ejecuté mi software antivirus
Otra [anchor]
Ninguna de las anteriores [anchor]

17. ¿Quién cree que debe tener la mayor responsabilidad para detener la diseminación de virus informáticos, correo electrónico fraudulento, spyware y spam? Seleccione todas las opciones que correspondan.

[Randomize]
Yo
El gobierno o los organismos de protección del consumidor
Proveedores de servicio de Internet y proveedores de servicio de correo electrónico
Vendedores de ordenadores y de software
Asociaciones profesionales
Empresas de software informático líderes
Fabricantes de ordenadores
Empresas de software antivirus
Sitios de redes sociales
Grupos de apoyo al consumidor
Otra [anchor]

18. ¿Cómo clasificaría la actuación de cada una de las siguientes entidades a la hora de detener los virus informáticos, el correo electrónico fraudulento, el spyware y el spam?

[Same order as Q17]
Yo
El gobierno o los organismos de protección del consumidor
Proveedores de servicio de Internet y proveedores de servicio de correo electrónico
Vendedores de ordenadores y de software
Asociaciones profesionales
Empresas de software informático líderes
Fabricantes de ordenadores
Empresas de software antivirus
Sitios de redes sociales
Grupos de apoyo al consumidor

Scale:
Muy buena
Bastante buena
Ni buena ni mala
Bastante mala
Muy mala

19. ¿Hasta qué punto está familiarizado con los términos “bot” o “botnet” con respecto al envío de spam y virus informáticos? [single response]

Muy familiarizado
Algo familiarizado
He oído hablar sobre el tema, pero no sé nada
Nunca he oído hablar de ello

20. ¿Sabe que hay virus maliciosos que pueden controlar su ordenador sin que usted lo sepa y que pueden utilizar su ordenador para diseminar spam o robar sus datos personales?

Sí
No

21. Un “bot” o “botnet” es un virus malicioso que puede controlar su ordenador sin que usted lo sepa y que puede utilizar su ordenador para diseminar spam o robar sus datos personales. ¿Qué probabilidades hay de que su ordenador se contagie con este tipo de virus?

[REVERSE SCALE ON ½ SAMPLE]
Extremadamente probable
Muy probable
Algo probable
Poco probable
Nada probable
No estoy seguro [anchor]

22. ¿Cómo puede saber si su ordenador ha tenido un “bot” o “botnet”? Seleccione todas las opciones que correspondan.

[Randomize]
Si mis amigos me dijeran que estaban recibiendo spam de mi dirección de correo electrónico
Si la compañía de mi tarjeta de crédito o mi banco me notificase sobre una actividad sospechosa en mi cuenta
Si mi software antivirus me alertase sobre su existencia
Si mi ordenador no funcionase normalmente o funcionase con mucha lentitud
Si aparecieran mensajes de error inusuales
Si observara archivos corruptos
Si viera un programa nuevo que yo no he instalado
Si aparecieran muchas ventanas emergentes
Otra [anchor]
No estoy seguro [anchor]

23. ¿Cuál de las siguientes entidades cree que tiene la responsabilidad de arreglar su ordenador si tuviera un virus, spyware o un bot/botnet? Seleccione todas las opciones que correspondan.

[Same order as Q17]
Yo
El gobierno o los organismos de protección del consumidor
Proveedores de servicio de Internet o de servicio de correo electrónico
Vendedores de ordenadores o de software
Asociaciones profesionales
Empresas de software informático
Fabricantes de ordenadores
Empresas de software antivirus
Sitios de redes sociales
Grupos de apoyo al consumidor
Otra [anchor]

24. Si descubriera que su ordenador se ha infectado, ¿cómo lo arreglaría? Seleccione todas las opciones que correspondan.

[RANDOMIZE]
Remotamente a través de mi proveedor de servicio de Internet o de mi proveedor de servicio de correo electrónico
Remotamente por un servicio de reparación de ordenadores
Remotamente por la empresa de mi software antivirus
Haciendo que un familiar o amigo se encargue de ello
Haciendo que un profesional venga a mi casa u oficina para su reparación
Llevando mi ordenador a un servicio de reparación
Lo repararía yo mismo
Otra [anchor]

25. ¿Cuál de los siguientes recursos utilizaría para informarse sobre el envío de spam y los "bots" o sobre cómo proteger mejor su ordenador? Seleccione todas las opciones que correspondan.

[RANDOMIZE]
Mi proveedor de servicio de Internet o mi proveedor de servicio de correo electrónico
La empresa de mi software antivirus
Motor de búsqueda o Internet
Familiar o amigo
Colega o compañero de trabajo
Asociaciones profesionales
Un servicio de reparación de ordenadores
Alguien del servicio o departamento de TI de mi empresa
El vendedor o fabricante de mi ordenador
Otra [anchor]
Ninguna de las anteriores [anchor]

Ahora tenemos algunas preguntas más con fines de clasificación.

26. ¿Qué tipo de sistema operativo tiene su ordenador personal?

Windows (cualquier versión)
Mac (cualquier versión)
Linux (cualquier versión)
Otro
No estoy seguro

27. ¿Cuál es su profesión o situación laboral? (MAY VARY ACROSS MARKETS)

Autónomo
Empleado a jornada completa
Empleado a media jornada
Jubilado
Labores del hogar
Desempleado
Estudiante
Otros

2009 Questionnaire

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?

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

NOTE: IN THE NEW IPSOS SURVEY, BEING AN EXPERT WILL NOT BE A REASON FOR TERMINATION

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.