Flash Eurobarometer

European Commission

EUROBAROMETER

Confidence in Information Society

Summary

Fieldwork: September 2008

Publication: May 2009

Flash Eurobarometer 250 – *The Gallup Organization*

This survey was requested by Directorate General Information Society and Media and coordinated by Directorate General Communication

Flash EB Series #250

Confidence in Information Society

Conducted by
The Gallup Organization, Hungary
upon the request of
Directorate General Information Society and Media

Survey coordinated by
Directorate General Communication

THE GALLUP ORGANIZATION

Table of contents

Introduction

This Flash Eurobarometer survey (#250) interviewed home internet users of the EU to appraise their confidence in the information society. Indeed, reliable and up-to-date statistical data on citizens' confidence in the information society are not available but are needed for effective and meaningful ICT security policy-making.

Because confidence is not a measurable feature, data indirectly reflecting confidence were selected; the survey gathered data to:

- evaluate the level of ICT security awareness / knowledge about potential and most typical risks
- quantify the ICT security-related damages experienced by home internet users (detected incidents, loss of money or time)
- know about the ICT security behaviour of (and measures taken by) the home internet users

The survey's fieldwork was carried out between 16 and 20 September 2008. Starting with a random sample of the general population aged 15 years and above, respondents were selected through a screening process. The eligibility criteria to be interviewed in the survey were that the persons must use the Internet from home at least once a month. After the selection process, **12.799** at-home internet users aged 15 years and above were interviewed in the 27 EU Member States. Please note, that persons who are probably users of the Internet, but do not have access at home, were not part of the target population because those who use the Internet from locations outside their home (i.e. Internet cafes or at work) are usually not responsible for ensuring the security of the equipment they use.

To estimate the EU average, results were weighted reflecting the number of home Internet users in each Member State based on Eurostat data (Romania, for example, despite its large population has relatively fewer internet users compared to countries with smaller population size, but significantly higher internet penetration rates.

Main findings

The reader should be reminded that there is a difference between the **perception** of security and the **actual level** of security. This report is meant to provide insights about confidence in the Information Society, but it does not answer to the question whether or not those who are confident indeed have the reason to feel secure. The reader is advised to bear this in mind: the **survey measured *attitudes* and because of the complexity of the issue it cannot provide a reliable picture on actual technical preparedness of respondents and their computer to counter the risks posed by internet activities.**

- Some Internet users in the EU have a **perception of security** that makes them confident that transactions over the Internet are safe. However, only 12% believe that these are *completely safe*, and 46% assume they are *rather* safe but **42% do not have confidence in these transactions.**
- One out of ten European Internet users believe that **online transactions are not safe** at all, and 19% believe that these are "not really" safe – including those who cannot tell whether such transactions are safe or not, almost four in ten users (39%) have significant doubts regarding Internet safety.
- **Users are very well informed about the existence** of typical threats. Computer viruses are the best-known hazards: virtually every Internet user confirmed to be aware of this potential danger (97% on EU-27 level).
- Consequently, **there are very few Internet users in the EU who say that they *do not* protect themselves against Internet-related security hazards[1].** Only a small minority of European Internet users agree that they do not implement (some) security measures because they do not feel threatened (10%), or because these are too expensive (7%) or because they don't know how to use them (6%).
- On the other hand, almost every Internet user in the European Union applies some **preventive technology** aimed to safeguard computers connected to the Internet and the data they store: 96% confirm using some antivirus, spam filter or firewall application. More than a third (35%) indicated that they (also) use alternative techniques to increase their safety while browsing the Internet.
- **Risk avoidance online behaviour** was also widely reported; users rarely give out personal data on the Internet (avoids as much as possible: 86%), and they rarely engage in peer-to-peer file transfers with people they don't know (81% indicate refraining from such activity). However, only a minority (although a very significant minority) do *not* carry out financial transactions over the Internet (42%).
- Despite the efforts users make in order to protect the privacy of their online communications and the integrity of their systems, many users have experienced **security problems in the past**. Looking at the past five years, 65% of EU Internet users reported being the victim of excessive spamming and 46% detected viruses on their computers. Considering all tested security problems, only about one in five (22%) of all EU Internet users reported that none of these problems were detected on their system.
- The security problems typically caused time loss for users, but harder-hitting **damages** were reported by relatively few of those who otherwise reported some security problem: Loss of non-personal data (e.g. damaged files, etc.) was the second most frequent result of Internet security

[1] The survey did not ask if the security products were indeed switched on, currently licensed to operate, regularly updated, etc. The survey did not ask separately the availability of anti-virus, firewall, and content filtering on the users' computers, as the primary objective was to get an insight about the users' *perception* of their safety.

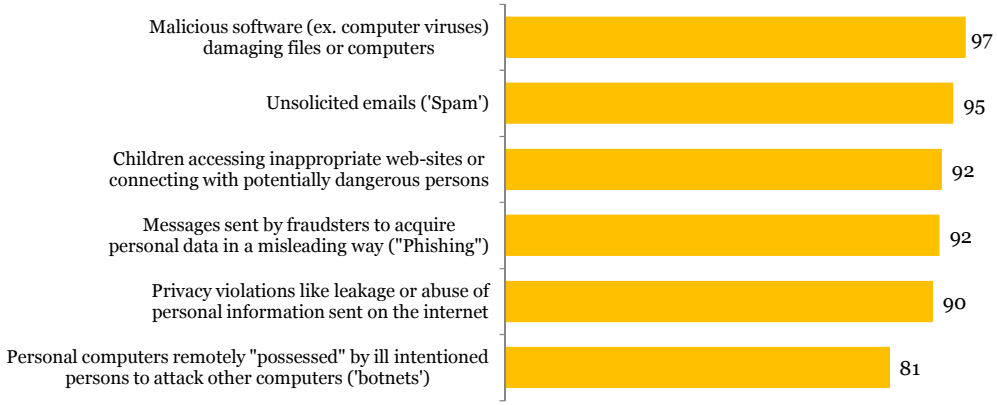
problems (18%). Only 16% of all internet users who encountered some security problem over the past five years also report direct financial losses (e.g. money stolen, computer repair costs, loss of valuable data).

- Three quarters of Internet users believe that they personally are **responsible** for ensuring their protection from Internet-related security hazards (75%). However, the majority of users also believe that their Internet service providers (52%) as well as those organisations that provide online services (51%) are also accountable for securing online transactions. Considerably fewer users feel that public authorities also have a responsibility regarding problems related to online security (31%).
- The survey asked Internet users if they would be interested in participating in practical **training course on Internet security**. Seven percent of all Internet users in the EU would consider attending such a course if it was offered for a charge, and 24% are open to the idea if this training were free. Overall, 67% of EU Internet users would not be willing to take part in such a course, mostly because they are confident that they know enough (31%); or on the contrary, they think that their current IT skill level is insufficient to meaningfully gain from such training (17%).

1. Awareness of online security hazards

Internet users seem to be well aware of the various hazards their online activity presents to them. Even the least known hazard (that of becoming a part of a 'botnet') was confirmed as something that more than eight out of ten users are already aware of.

Awareness of the existence of security problems related to Internet usage



Q2. Are you aware of the existence of the following security problems related to internet usage?
Base: all respondents
% of 'Yes', EU27

As the graph above illustrates, computer viruses are the best-known hazards the Internet presents to one's computer and digitally stored data. Virtually every Internet user confirmed that they are aware of this potential danger (97% on EU-27 level). The second most frequently recognised problem is that of spam, with 95% confirming that they are aware that unsolicited emails are often sent to email account holders. Ninety-two percent of EU Internet users are aware that there are added potential dangers if a child is browsing the Internet (inappropriate content or contacts with potentially dangerous persons), and the same proportion is aware that users' personal information might be obtained fraudulently, via phishing. Nine out of ten users are conscious that their privacy may be violated by an abuse of their personal information sent via the Internet (90%). Finally, as indicated, 81% claim to be aware that there computer may be part of a botnet.

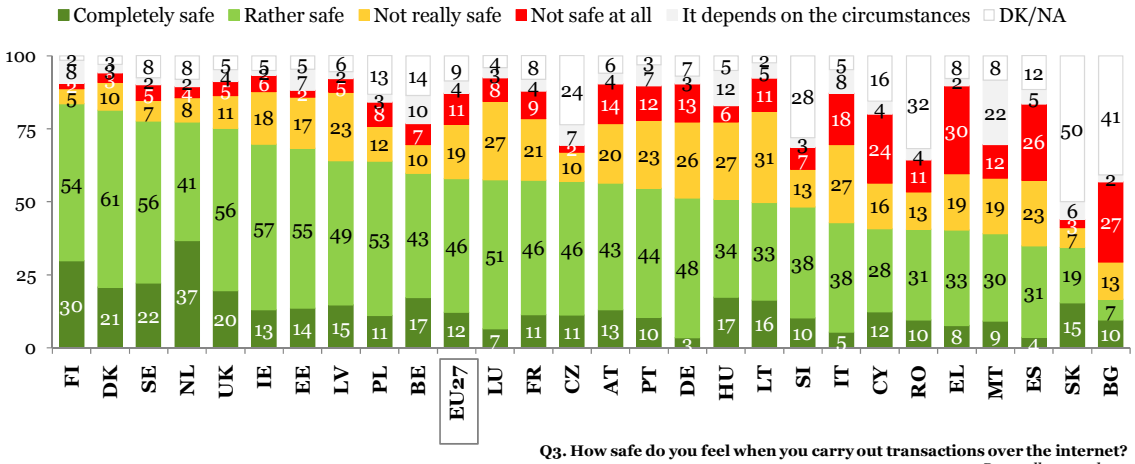
Country variations, as one can expect with such high figures, are only slight (as detailed below). EU Internet users are generally aware of the potential hazards regardless of the country of residence

2. Confidence in Internet transactions

While most Internet users in the EU are confident that transactions over the Internet are safe (12% believe that these are *completely safe*, and 46% assume they are *rather* safe, totalling 58%), there is a significant minority of users who do not have confidence in these transactions. One out of ten European Internet users has the opinion that such transactions are not safe at all, and 19% believe that these are not really safe – and if we add those who can't tell whether such transactions are safe or not (9%), almost four in ten users (39%) have significant doubts regarding Internet safety in this regard. Four percent of respondents indicated that the safety of the transaction depends on its nature ('it depends on the circumstances').

Confidence in Internet transactions is the highest in the Nordic Member States (Finland: 84% consider them *rather* or *completely* safe; Denmark: 82%; Sweden: 78%), but the vast majority of Dutch (78% - also with the highest proportion of 'completely safe' replies: 37%), British (76%), Irish (70%) and Estonian (69%) users also trust the safety of Internet transactions

Confidence in internet transactions



Q3. How safe do you feel when you carry out transactions over the internet?
Base: all respondents
% by country

2

On the other hand, confidence levels are lowest in Bulgaria (17%) and Slovakia (34%); in Slovakia people are most likely not to provide their opinion, stating that they 'do not know' how safe transactions over the Internet are (55%). The situation is similar in Bulgaria (don't know: 41%), but Bulgaria is among the three Member States where people with low or no confidence (40% in total) outnumber those users who fundamentally trust (as indicated, 17%) transactions over the Internet. Results are similar as well in Spain (trust: 35%, do not trust 49%) and in Greece (trust: 41%, do not trust 49%).

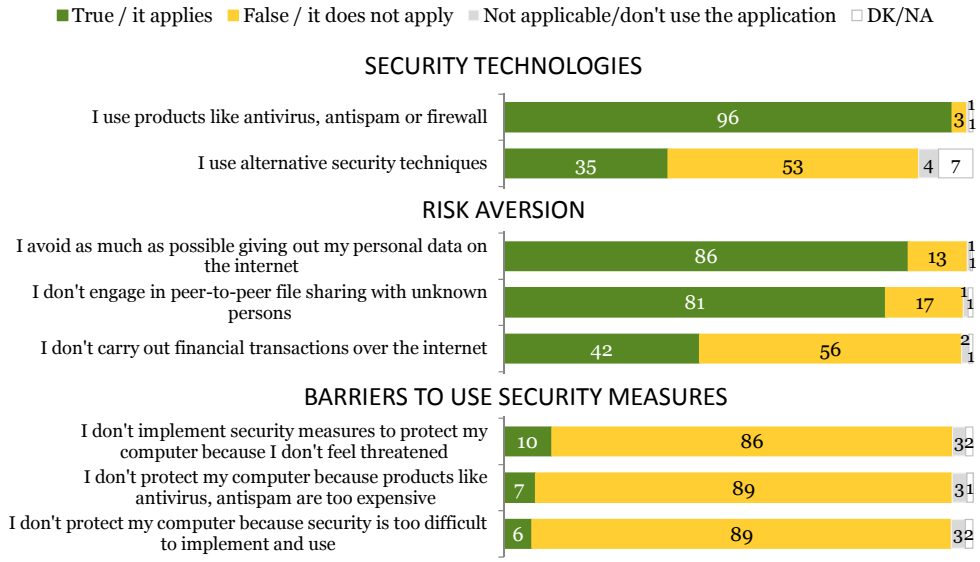
Daily Internet users are significantly more confident than those who use the web less regularly (62% vs. 48%), and the gap is similar between those with a degree and those with only a basic education (64% vs. 48% respectively). Men are more confident about the safety of online transactions (62%) than women (55%), while there is no clear pattern among the various age groups or the segments defined by level urbanisation.

[2] Due to technical reasons, as a result of rounding, the sums in charts in a few case do not add up to 100%.

3. Security precautions

Almost every Internet user in the European Union applies some preventive technology aimed at safeguarding computers connected to the Internet and the data they store: 96% confirm using some antivirus, antispam or firewall application. More than a third (35%) indicated that they also use further solutions to increase their safety while browsing the Internet. Only a small minority of European Internet users agree that they do not implement (some) security measures because they do not feel threatened (10%), because these are too expensive (7%) or because they don't know how to use them (6%).

Precautions aimed to increase internet security



Q4. I will read a list of possible actions / behaviours resulting from real or perceived risks of the internet. For each of these please tell me which applies to you and which does not?
Base: all respondents
% EU27

3

Standard security technologies (such as antivirus software, spam filters and firewalls) are standard accessories on home computers throughout the European Union, most users report that their systems are equipped with at least one of these. Ninety percent or more of users confirmed this to be the case in 24 Member States, the most affirmative responses came from Portugal and France (98% both). The three Member States with less than 90% confirming the usage of standard security technologies are Bulgaria (89%), Romania (85%) and Cyprus (82%).

Daily users of the Internet are somewhat more likely to report using such standard Internet security technologies (97%) compared to those who are less regularly online (93%), and those with degrees are also more likely to apply such technologies (97%) than those with medium (95%) or basic (91%) education.

Various **alternative** or complementary security techniques and technologies are available for the more security-conscious user to improve the security of computer systems and online communication / data exchange (examples of such techniques: not using mainstream software products, disconnecting WiFi when not behind the computer, avoiding giving personal data, refusing financial transaction on service that do not offer a hardware security, setting the browser parameters to values ensuring security, avoid to browse potentially dangerous website,…). Such techniques are used by about half of the users in

[3] Due to technical reasons, as a result of rounding, the sums in charts in a few case do not add up to 100%.

Portugal (51%) and Cyprus (50%). On the other hand, these are significantly less popular in Finland (19%), Austria (20%), France and Lithuania (21% both).

The difference between daily and less regular users is even more pronounced in this aspect (38% of the former group uses alternative security technologies versus 28% of the latter). Those between 15 and 24 years of age and those with a higher education are also more likely than the average to use such solutions (38% and 37%, respectively).

Risk avoiding behaviour is also widely reported; users rarely give out personal data on the Internet (avoids as much as possible: 86%), and they equally rarely engage in peer-to-peer file transfers with people they don't know (81% indicate refraining from such activity). Only a minority (however a very significant minority) do not carry out financial transactions over the Internet (42%).

The most widespread risk aversive behaviour detected by this survey is that users are **reluctant to give out personal information** in Internet-based transactions. Relatively speaking, Czech users were the least intent on keeping their personal data private in Internet transactions, but even in the Czech Republic, 75% confirmed that they are reluctant to transmit personal data in online transactions. There are only very slight variations in this aspect if one looks at the various user groups. Especially the eldest group (89%) and those who are not online every day (90%) avoid transmitting personal data in online communication.

Peer-to-peer file exchanges with strangers are avoided, once again, by most EU Internet users; a large number of them confirm that they do not engage in such activities. This is especially the case in Estonia (92%), Finland, Slovenia and Greece (90% each), see graph on the next page. On the other hand, only 53% of Danish Internet users indicated that they do not share files with strangers. Age plays an important role in determining if one does or does not engage in file sharing: 86% of those aged 55 or above state that they do not exchange files with strangers, while this proportion is 74% among the 15-24 year olds.

As a precaution, especially Bulgarian, Greek (66% both) and Hungarian (65%) Internet users **do not perform financial transactions online**, but also in Romania (58%), Spain (56%) and Italy (55%) the majority of Internet users avoid paying or dealing with their bank in an online environment. On the other hand, only one in ten users in Finland indicated that they do not carry out online financial transactions (11%), and those in Estonia (26%), UK (27%), Sweden and the Czech Republic (30% both) are also significantly less likely than the average EU Internet user to report that they do not use the Internet for bank transactions or payments.

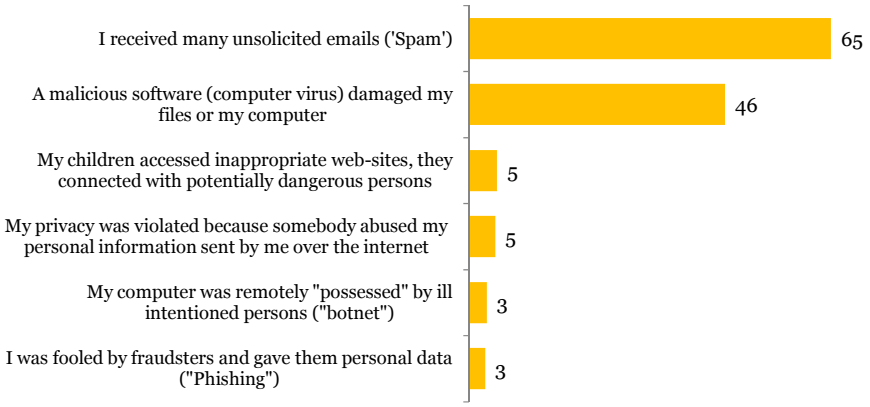
In this aspect various user groups follow clearly different conduct: those who use the Internet on a daily basis are much more likely to carry out financial transactions online (do not: 38%) compared to those who use the web less regularly; in the latter group 52% indicated that they do not pay anything online. There is a significant gap between the two genders, as well: men are more likely to pay or bank online (39% replied that they don't), while the ratio of those not engaging in such transactions is 44% among women. Lastly, young (15-24: 47%) and non-working users (46%) were also more likely than most to claim that they do not carry out online transactions, probably partly due to security concerns as well.

Curiously, those using standard security technologies are more likely to detect (79%) at least one of the security breaches tested than those who do not apply such techniques (58%). Obviously, those who apply e.g. anti-virus software are more likely to notice virus-related problems (e.g. when installing the software or when updating it) compared to those who do not. In other words, the above results suggest that the application of security technologies do not only prevent security breaches, but they also help detecting those that would have otherwise gone unnoticed.

4. Security problems faced

Despite the reported efforts users make in order to protect the privacy of their online communications and the integrity of their systems, many of them have encountered security problems in the past. Over the past five years, 65% of EU Internet users reported being the victim of excessive spamming and 46% detected viruses on their computers.

Security problems detected



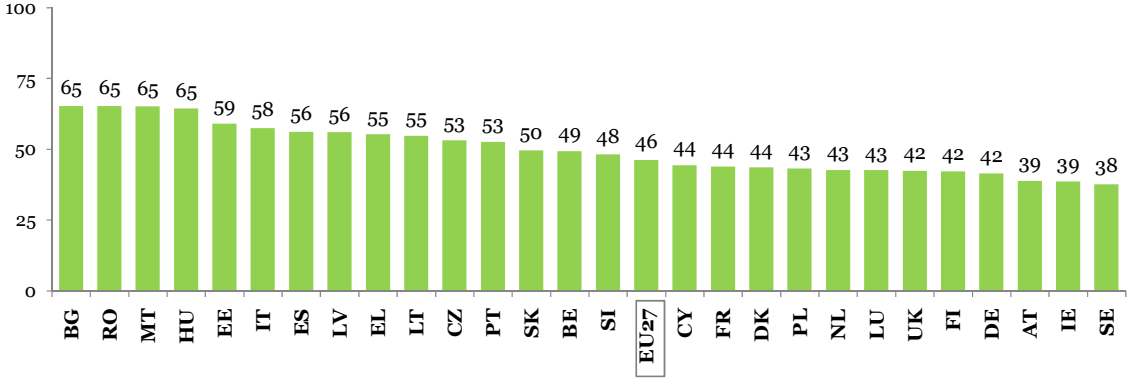
Q5. Did you have any of the following security problems using the internet in the last five years?
Base: all respondents
% of 'Yes', EU27

Reports of other security problems are relatively low, but due to the nature of these problems many of them might go unnoticed. Five per cent of users indicated that their privacy was violated by the abuse of personal information that they sent online, 5% are aware of their children having accessed inappropriate content or having come into contact with potentially dangerous persons. Three per cent are aware of their computer having become part of a botnet, and the same proportion indicated that they unintentionally provided fraudsters with their personal data.

Almost two thirds of all Internet users in Bulgaria, Malta, Romania and Hungary (65% each) reported that they have **detected a virus infection** on their computer during the past 5 years.

Virus infection

A malicious software (computer virus) damaged my files or my computer (ex. My computer was not working anymore or was working very slowly, I was always re-directed to a website I did not choose)



Q5. Did you have any of the following security problems using the internet in the last five years?
Base: all respondents
% of 'Yes', by country

Even in those countries where relatively few users reported detected virus infections, this problem affected a significant number of users: 38% in Sweden, 39% in Ireland and Austria.

Intensive usage implies more infections: those who are online every day are much more likely to report such incidents (50%) compared to those who use the Internet less regularly (39%).

There is a clear link between age and the likelihood of virus infection; the older the user is the less likely he or she is to indicate the detection of a virus (59% of those 15-24 years old had detected a virus, while this proportion was only 33% among users 55 and older). Men were also more likely than women to indicate that their computer had at some point become contaminated (50% vs. 43%, respectively).

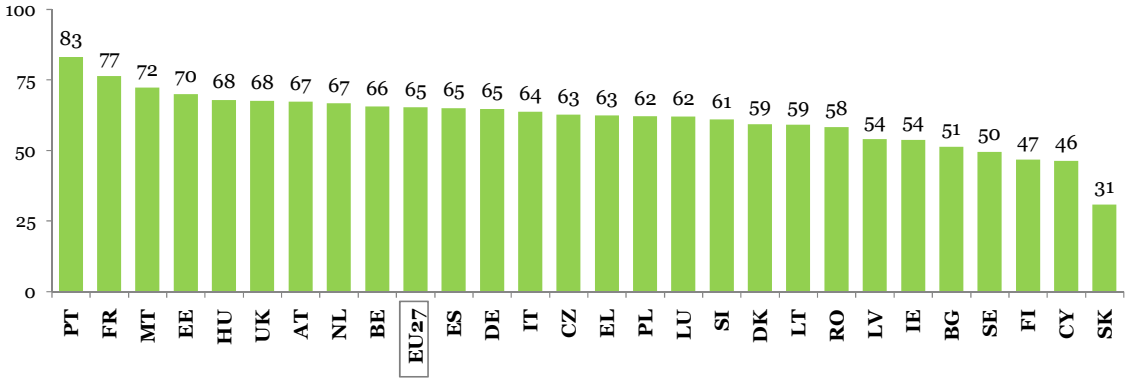
Excessive spamming affects the majority of Internet users in most Member States. Receiving large amounts of unsolicited emails was most often reported in Portugal (83%), France (77%) and Malta (72%). Countries where less than half of the users complain about this problem are Slovakia (31%), Cyprus (46%) and Finland (47%).

Spam emails are received by most users in all segments, however some segments stand out: those who use the Internet on a daily basis (69% reported excessive spam vs. 'only' 56% of the less regular users), the self-employed (74%, vs. e.g. 61% of those who do not work) and men (68% vs., 63% among women).

There is a clear relation between educational attainment and the amount of spam received: 71% of those who completed higher education, 61% with a secondary school diploma and 57% with a primary education indicated the reception of large amounts of spam. The tendency is similar regarding levels of urbanisation: metropolitan users are more likely to be spammed (69%) than are those in smaller cities (65%) or villages (64%).

Excessive spam

I received many unsolicited emails ('Spam')



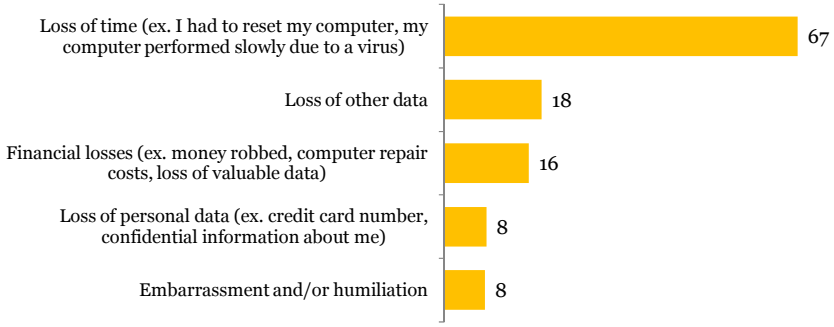
Q5. Did you have any of the following security problems using the internet in the last five years?
Base: all respondents
% of 'Yes', by country

5. Damages suffered

While this survey did not attempt to explore and estimate the volume of financial and other losses related to online security, respondents reporting security problems from the past five years were asked to say whether or not they suffered damages typically related to Internet use.

The most often mentioned consequence of Internet security problems was the loss of time, specifically because of virus infections (slow systems, time needed to reinstall, etc.). Two thirds of those in the EU who experienced security problems indicated this. Loss of non-personal data (e.g. damaged files, etc.) was the second most frequently reported result of Internet security problems, although at a significantly lower rate; 18% in the EU27 level claimed such damage. The proportion of those who reported direct financial losses (e.g. money stolen, computer repair, loss of valuable data) is similar: such issues were reported by 16% of all Internet users in the EU who encountered some security problem over the past five years.

Damages suffered



Q6. What damages have you experience?
Base: who had any security problem in the last five years
% of 'Experienced', EU27

Internet users are, however, much less likely to indicate that they suffered a loss of personal data (credit card number, etc. - 8%) and they are similarly unlikely to have suffered psychological damage related to Internet security problems (e.g. embarrassment or humiliation, 8%).

In order to clarify the harmfulness of various security breaches, reports of any actual damage were analysed by the type of security problems experienced. Although a single user might have experienced more than one security problem during the past five years and therefore misreported damages as resulting from a problem other than that from which they came, this analysis helps us understand the relative hazard levels associated with each of the security problems investigated in this survey.

Security problems and inflicted damages
(%, EU-27)

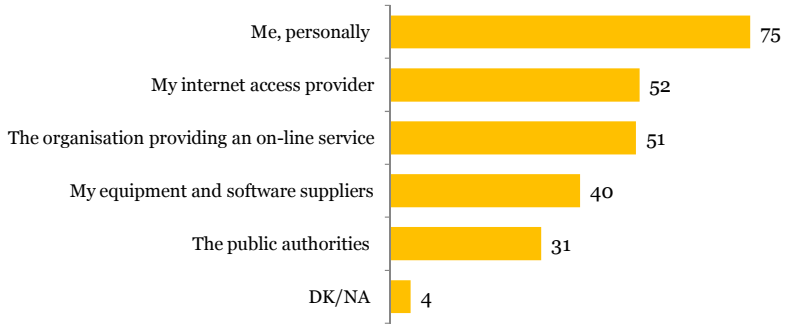
	ANY DAMAGES	
SECURITY PROBLEMS:	yes	no
Virus infection	44	56
Phishing	51	49
Abuse of personal data	54	46
Spam	30	70
Children	53	47
Botnet	64	36

As the table above shows, those who received spam are the least likely to mention that they suffered any damage related to Internet security issues (30%), and the majority of those who indicated a virus infection did not actually suffer damages at all (56%). The most potent hazards are related to the instances of botnet activity: 64% of the EU Internet users who noticed such a security breach confirmed that they suffered some damage related to Internet security issues. Also, the majority of those who were victims of phishing (51%), abuse of personal data (54%), or reported security problems related to children using the Internet (53%) confirm that they suffered damages related to online security issues.

6. Responsibility for Internet security

EU Internet users recognize a shared responsibility for protecting users from security problems, with the users themselves taking the lead: three quarters of Internet users believe that they personally are responsible for ensuring their protection from Internet-related security hazards (75%). However, the majority of users also believe that their Internet service providers (52%) as well as those organisations that provide online services (51%) are also accountable for security breaches in online transactions.

Taking responsibility for ensuring security on the Internet



Q7. Who, in your opinion, is responsible for ensuring your security on the internet?
Base: all respondents
% of 'Mentioned', EU27

Four in ten users (40%) feel that responsibility also lies with the hardware and software providers to create secure systems that resist malicious attempts to target users or their computers. Lastly, 31% feel that public authorities also have a responsibility in protecting people from problems related to online security.

In 21 Member States, the three most frequently given replies were those which are the most frequent at the EU-27 level as well, and are also generally given in the same order.

In every user group we see the pattern reflecting the EU average; respondents place themselves in the first place, they then hold Internet service providers and online service providers accountable for ensuring the safety of online activities, more or less equally.

While there is no variation in the rankings, there are some differences in the level of affirmative answers **by user groups**. Those between 15 and 24 years were more likely than any other age group to lack an opinion, and the least likely to indicate each of the answer categories provided. However, those with higher levels of education are the most likely to indicate responsibility for *each* agent, and least likely to claim that they have no opinion.

Personal responsibility was confirmed especially in the segment that completed higher education (81%), while only 68% of those with only a primary education felt that they were responsible for

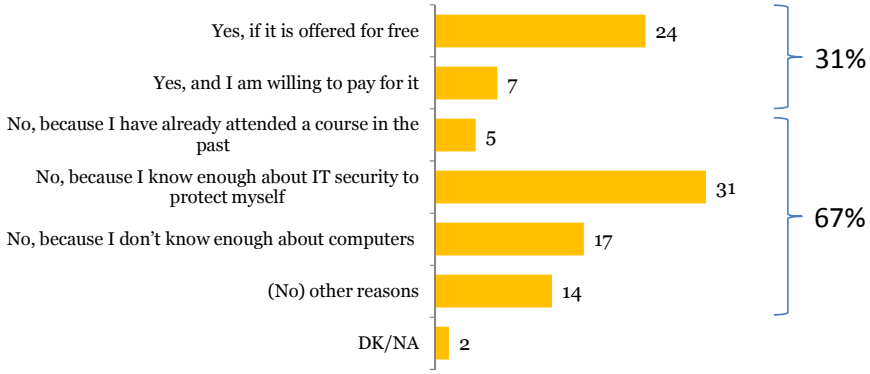
ensuring their security on the Internet. Men were more likely than women (77% vs. 74%) to assume personal responsibility, as were white and blue collar employees (77% both) compared to the self-employed (74%) and non-working Internet users (72%).

Public authorities are in turn more likely to be held responsible by women (33% vs. 30% of men), by the self-employed (32%), by white-collar employees (33%), and by those aged 40-54 (35%). Also, metropolitan users are more likely to call for public protection with regard to Internet security (33% vs. 29% in rural areas.)

7. Improving Internet security skills

The survey asked Internet users if they would be interested in participating in a practical training course on Internet security. Seven percent of all Internet users in the EU would consider attending such a course if it were offered for a charge, and 24% are open to the idea if this training were free. Overall, 67% of EU Internet users are not at all willing to take part in such a course, mostly because they are confident that they know enough already (31%). The most likely to have this opinion were the German (40%), Austrian (38%), British and Danish (37%) users.

Propensity to participate in a course on IT Security



Q8. Would you consider participating in a few hours' course on IT Security to increase your knowledge on security when you use the internet?
Base: all respondents, please note that numbers do not exactly add up due to rounding
% EU27

Looking at other reasons for not wanting to participate in an Internet security training course we note that five per cent indicated a lack of interest because they already received training in this subject (Hungarian users are the most likely to select this option: 12%). Seventeen per cent think that their current *general* IT skill level is insufficient to gain any meaningful knowledge from such training. This opinion is most likely to be held by Slovak (33%), Polish (25%) and Hungarian (23%) users. Finally, 14% indicated other reasons to explain their lack of interest in a training course of this sort.

The highest proportions of those who would be willing to participate in security courses are in Bulgaria (61%), Cyprus (59%) and Greece (52%), where more than half the users would attend (at least a free-of-charge) training course on Internet security. Twenty-seven per cent of Bulgarians and 25% of Cypriot Internet users would even be willing to pay for such a course. On the other hand, Dutch (14%), Czech (20%) and Italian (23%) users are the least interested in this training opportunity, even if it were free.

The openness to participation in this theoretical course varies only very slightly across user segments. Those who emerged as the most interested - those aged 25-39 years (36%) and women (34%) - are only slightly more attracted to the idea compared to the 32% EU average. Those willing to pay for such training were most likely to be self-employed users (10%).