



G Data

## Security Survey 2011

How do users assess threats on  
the Internet?

Go safe. Go safer. **G Data.**



# Contents

<b>1 Summary</b> .....	<b>2</b>
1.1 Scope and purpose of the survey .....	2
1.2 How aware are surfers of threats on the Internet? .....	2
<b>2 Methodology of the survey</b> .....	<b>3</b>
<b>3 Results of the G Data Security Survey 2011</b> .....	<b>4</b>
3.1 How are users protecting themselves against attacks?.....	5
3.1.1 How do users assess the effectiveness of free virus protection solutions? .....	6
3.1.2 Number of unprotected PCs .....	8
3.1.3 Suite or just virus protection? .....	9
3.2 Where do web surfers expect there to be the most threats? .....	11
3.2.1 The eleven myths of Internet security .....	11
3.2.2 Who is better informed: younger or older Internet users? .....	16
3.2.3 In which country are Internet users best informed of the risks? .....	18
3.2.4 Are men the 'safer' surfers?.....	19
3.3 Behaviour on social networks .....	20
3.3.1 Who's safer on social networks: men or women? .....	22
3.3.2 Who behaves more safely on social networks: younger or older users? .....	22
<b>4 Conclusions</b> .....	<b>24</b>
<b>Appendix</b> .....	<b>26</b>
G Data Software AG.....	26
Survey Sampling International.....	28
Glossary .....	28

# 1 Summary

## 1.1 Scope and purpose of our research

Every day we see reports about new attacks on Internet users and companies, about data theft, new computer malware and the formation of eCrime cartels. Meanwhile, consumers increasingly find themselves to be the target of the same kind of offenders and criminals, running an ever-higher risk of becoming the victims of global bands of cyber criminals. Clearly, in the age of the Internet, protecting one's digital identity has become an issue of fundamental significance for all sectors of society and there is a huge range of IT security solutions available for protecting personal computers. But just how well informed are Internet users about the genuine threats on the Internet and the perpetrators' methods? Are younger or older users more astute in terms of IT security – and indeed, are men or women 'safer' Internet users? In this global 2011 Security Survey, we take a look at these and many other questions, putting IT security myths to the test and showing how users really assess threats on the Internet.

## 1.2 How aware are surfers of threats on the Internet?

The results of the G Data 2011 Security Survey, i.e. individual awareness and assessment of threats, were compared with the actual threat situation. The analysis shows that the level of awareness among Internet users is still inadequate and out of date in many respects.

Almost all survey participants have a general notion of the threats lurking on the Internet and they try to safeguard their PCs against them accordingly. However, this knowledge rarely reflects a realistic view of the actual threats. Therefore, nine out of ten PC users assume that they will notice if they have a malware infection. In the opinion of survey participants, this will be evidenced by peculiar pop-ups, slow computer performance or because the computer no longer works at all. The majority of survey participants are convinced that at least one of these symptoms will occur.

However, the aim of online criminals is to earn as much money as they can, which means that they want to keep infections hidden from users for as long as possible. Generally speaking, all data such as credit card information, bank details, access data for online shops and e-mail accounts, etc. is stolen on the initial infection. Then the computer is usually linked to botnets, which are rented out in underground forums as spam 'spray guns' or for DDoS attacks, without the user realising.

Cyber criminals have been using social networks to distribute malware for a long time, in order to publish links to primed websites. While distribution via spam e-mail and infected file attachments certainly still occurs, this is now the secondary distribution path, despite what many survey participants believe. In the distribution concepts for computer malware, spam is used to lure recipients to malicious websites and then infect their PCs via drive-by download (see section 3.2.1: The eleven myths of IT security - and where Internet users are wrong).

There is an immense level of trust among social network users: 35 percent trust links published within their network and some 19 percent click on links, regardless of where they come from, thereby making themselves easy targets for cyber criminals and their illegal activities.

So how are users protecting themselves against attacks? The good news is that only 11 percent of all Internet users log on to the Internet with virtually no protection, i.e. they completely do away with functional antivirus solutions or Internet security packages. 48 percent of survey participants use

free antivirus programs and therefore do not bother with a separate firewall, HTTP protection, CloudSecurity, anti-spyware or anti-spam modules. Rather, over 50 percent of these users assume that they have installed a complete software package that includes these essential protection technologies (see section 3.1: How are users protecting themselves against attacks?).

In summary, the G Data 2011 Security Survey shows that users are incorrectly assessing the real threats on the Internet and that a large percentage of private users are not adequately protecting their computers. The consequences of this are obvious: too many people are running the risk of their computer becoming infected with malware without their knowledge. This lack of knowledge plays into the hands of both cyber criminals and malware authors.

## 2 Methodology of the survey

The G Data 2011 Security Survey entitled "How do users assess threats on the Internet?" is based on an international online survey in which 15,559 Internet users in eleven countries between the ages of 18 and 65 took part. Survey participants answered questions on the subject of online threats on the Internet, surfing behaviour, use of security solutions and their awareness of security on the Internet. A separate web page was set up for each country in its own language with an identical set of questions for the survey. All participants had their own PC and Internet access. The data was recorded in February and March 2011 and analysis carried out by Survey Sampling International<sup>1</sup> under contract to G Data Software AG. The data was then assessed and analysed in April and May 2011.

Table 1: Age distribution and sex of the participants

Age	Men	Women	Total
18-24	1273	1430	<b>2703</b>
25-34	1636	1796	<b>3432</b>
35-44	1603	1784	<b>3387</b>
45-54	1585	1647	<b>3232</b>
55-64	1381	1424	<b>2805</b>
<b>Total</b>	<b>7478</b>	<b>8081</b>	<b>15559</b>

Table 2: Participants by country

Country	Men	Women	Total
Austria	343	425	<b>768</b>
Belgium	432	496	<b>928</b>
France	582	622	<b>1204</b>
Germany	591	603	<b>1194</b>
Italy	575	563	<b>1138</b>
Netherlands	336	367	<b>703</b>
Russia	503	582	<b>1085</b>
Spain	579	579	<b>1158</b>
Switzerland	346	333	<b>679</b>
United Kingdom	545	561	<b>1106</b>
United States of America	2646	2958	<b>5604</b>
<b>Total</b>	<b>7478</b>	<b>8081</b>	<b>15559</b>

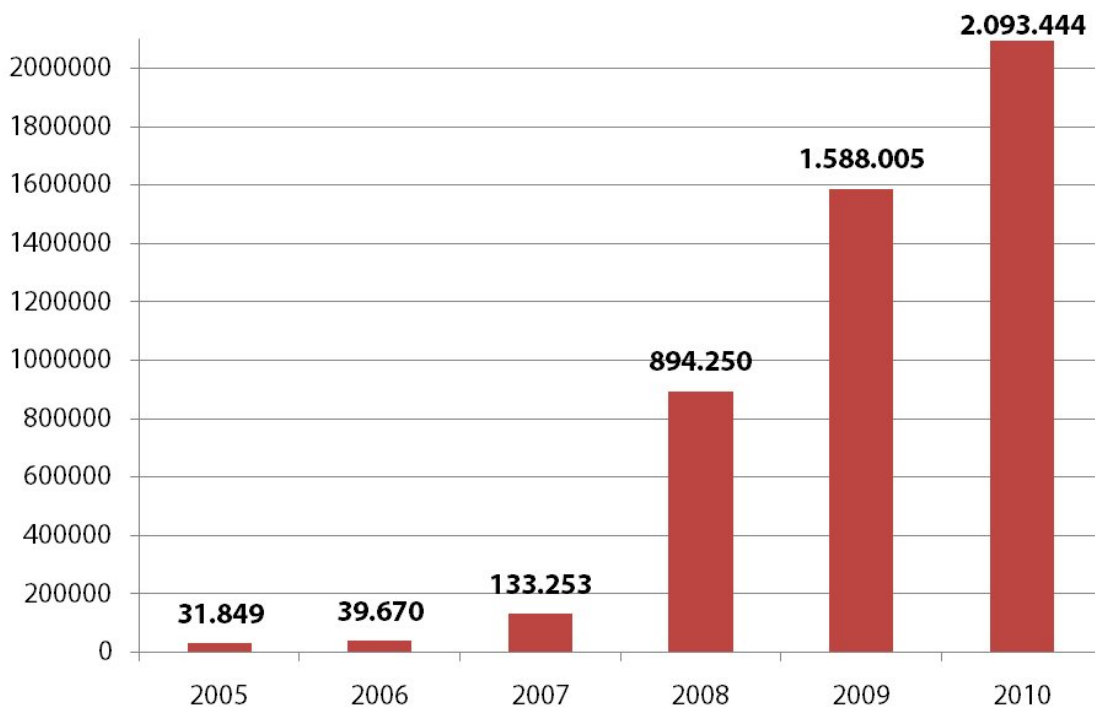
<sup>1</sup>Additional information on Survey Sampling International is available in the appendix.

### 3 Results of the G Data 2011 Security Survey

Attacks on companies and private users have increased significantly in recent years. Online criminal activity has become a profitable business, and perpetrators are using a wide range of methods of attack to infect computers with malware and to steal every conceivable type of data from victims and resell it for a profit.

In the past year alone, G Data has recorded more than two million new malware programs for Windows systems.<sup>2</sup>

Diagram 1: Number of new malware programs per annum since 2005



Malware is distributed by criminals in a number of ways. One option is to hide malware programs on web pages. Simply visiting a compromised web page is enough to enable so-called drive-by downloads, which infect computers with viruses, Trojans, spyware and other malware. Users encounter such malicious web pages either when they are surfing the Internet or when the perpetrators publish the URLs on social network platforms or in messages in chat rooms. Online criminals also continue to use spam e-mail to lure users into clicking on links to primed websites or into opening infected file attachments. In this case the e-mail content refers to anything from an alleged invoice, a warning or exclusive photos to a current event, etc. If users follow the request they are taken straight to the malicious website, where they may unwittingly pick up a malware program.

Users can only protect themselves against the threats they are exposed to by employing a comprehensive security solution and treating the medium of the Internet with caution.

<sup>2</sup>See G Data Malware Report 2/2010, <http://www.gdatasoftware.com/information/security-labs/information/whitepaper.html>

### 3.1 How are users protecting themselves against attacks?

The result of the G Data 2011 Security Survey shows that out of over 15,500 users questioned, more than 89 percent have security software installed on their system, of which 48 percent are relying on free software.

Diagram 2: What security solution have users installed on their systems?

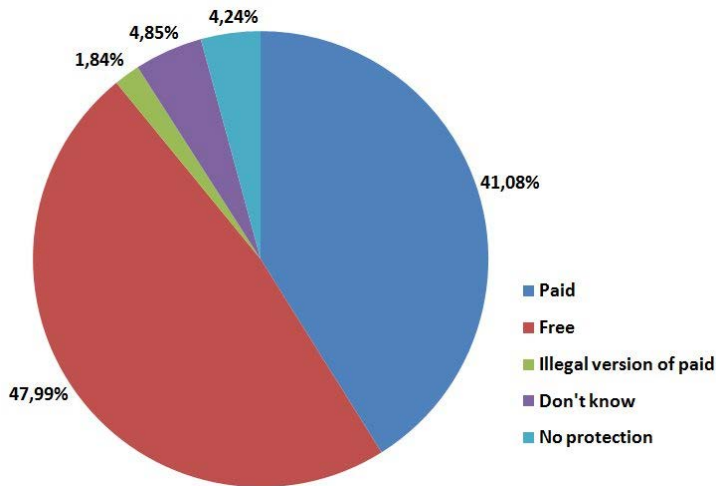


Table 3: Results for the question: what security solution have users installed?

Which security software do you use?					
	Paid	Free	Illegal version of paid	Don't know	No protection
Men (18-24)	39,83%	43,99%	4,08%	4,87%	7,23%
Men (25-34)	42,60%	47,37%	2,14%	2,87%	5,01%
Men (35-44)	42,98%	47,16%	1,62%	3,93%	4,30%
Men (45-54)	42,15%	50,41%	1,32%	2,84%	3,28%
Men (55-64)	44,97%	48,08%	1,16%	2,68%	3,11%
<b>Total Men</b>	<b>42,55%</b>	<b>47,53%</b>	<b>2,01%</b>	<b>3,40%</b>	<b>4,52%</b>
Women (18-24)	34,69%	51,47%	2,10%	6,08%	5,66%
Women (25-34)	40,81%	47,05%	2,62%	5,57%	3,95%
Women (35-44)	42,60%	46,92%	1,51%	5,44%	3,53%
Women (45-54)	40,80%	48,33%	1,09%	6,86%	2,91%
Women (55-64)	38,48%	49,02%	1,05%	7,30%	4,14%
<b>Total Women</b>	<b>39,71%</b>	<b>48,41%</b>	<b>1,70%</b>	<b>6,20%</b>	<b>3,98%</b>
<b>Total</b>	<b>41,08%</b>	<b>47,99%</b>	<b>1,84%</b>	<b>4,85%</b>	<b>4,24%</b>

In comparison to the overall result of the Security Survey, the United Kingdom stands out as being above average: over 94 percent of those surveyed use a security solution. Russia has the lowest proportion with almost 83 percent. Therefore, at least four out of five survey participants in individual countries consistently use security software.

Diagram 3: What security solution have users in individual countries installed on their systems?

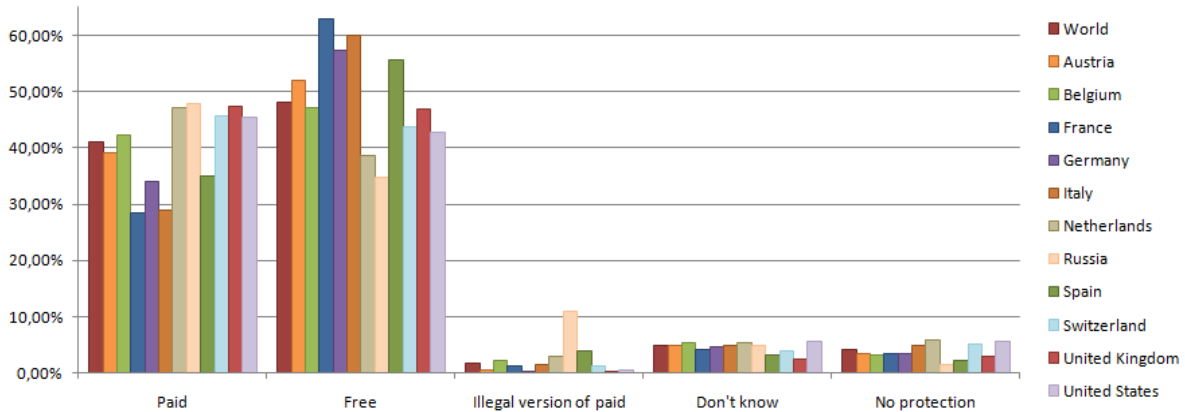


Table 4: Results by country in detail: what security solution do users have installed?

Which security software do you use?					
	Paid	Free	Illegal version of paid	Don't know	No protection
World	41,08%	47,99%	1,84%	4,85%	4,24%
Austria	39,19%	51,95%	0,52%	4,95%	3,39%
Belgium	42,24%	47,09%	2,16%	5,39%	3,13%
France	28,41%	62,79%	1,16%	4,24%	3,41%
Germany	34,09%	57,37%	0,34%	4,77%	3,43%
Italy	28,82%	60,01%	1,40%	4,92%	4,83%
Netherlands	47,23%	38,55%	2,99%	5,41%	5,83%
Russia	47,83%	34,84%	10,97%	4,79%	1,57%
Spain	34,96%	55,57%	4,00%	3,22%	2,26%
Switzerland	45,76%	43,80%	1,26%	3,92%	5,26%
United Kingdom	47,29%	46,84%	0,27%	2,53%	3,07%
United States	45,40%	42,74%	0,55%	5,71%	5,60%

Users can combine free antivirus software with other free tools. However, the potential incompatibility between individual programs and the security solution installed can cause problems.

In addition to virus protection, important components for effectively protecting a computer include a personal firewall, a spam filter and, last but not least, suitable web protection. In this regard, G Data offers a free browser plug-in, G Data CloudSecurity, which is compatible with all antivirus solutions.<sup>3</sup>

### 3.1.1 How do users assess the effectiveness of free virus protection solutions?

As stated above, the entry points at which an infection can get into a PC vary. Modern security solutions should provide protection from such threats. Taken individually, free antivirus programs are not in a position to do so. This is because they do not contain the protection technology that is vital for comprehensive protection. This includes anti-spam, web filter, firewall, and behaviour-based recognition of malware and Cloud security.

<sup>3</sup> Additional information on free web protection can be found at: <http://www.free-cloudsecurity.com>

Against this background, users were asked about their view of the scope of service and quality of free protection programs. Almost 44 percent of survey participants regard the scope of service and quality of free security software as equivalent to purchased solutions.

Diagram 4: Assessment of effectiveness: is free security software as good as purchased security solutions?

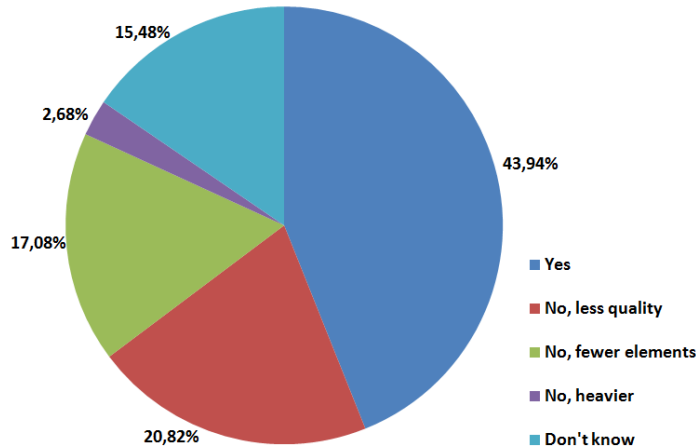


Table 5: Results of the question in detail: Do users regard free and purchased security solutions as equivalent in terms of quality and scope?

Is free security software as good as paid for software ?					
	Yes	No, less quality	No, fewer elements	No, heavier	Don't know
Men (18-24)	42,42%	25,69%	17,67%	2,83%	11,39%
Men (25-34)	46,03%	23,96%	17,30%	3,30%	9,41%
Men (35-44)	45,60%	22,46%	17,90%	2,87%	11,17%
Men (45-54)	42,84%	22,02%	19,05%	2,52%	13,56%
Men (55-64)	42,87%	20,71%	19,48%	2,32%	14,63%
<b>Total Men</b>	<b>44,06%</b>	<b>22,92%</b>	<b>18,27%</b>	<b>2,78%</b>	<b>11,97%</b>
Women (18-24)	43,64%	22,10%	17,97%	2,45%	13,85%
Women (25-34)	44,82%	21,27%	16,31%	3,29%	14,31%
Women (35-44)	43,39%	20,74%	15,92%	2,30%	17,66%
Women (45-54)	43,47%	16,03%	15,48%	2,19%	22,83%
Women (55-64)	43,75%	13,55%	14,26%	2,67%	25,77%
<b>Total Women</b>	<b>43,83%</b>	<b>18,87%</b>	<b>15,99%</b>	<b>2,59%</b>	<b>18,72%</b>
<b>Total</b>	<b>43,94%</b>	<b>20,82%</b>	<b>17,08%</b>	<b>2,68%</b>	<b>15,48%</b>

France comes out on top, when the countries are compared: 53 percent of those asked see no difference between free and purchased security solutions. In comparison, Dutch respondents had the lowest score - barely 35 percent consider free and purchased security software to be equivalent.

Diagram 5: Assessment of the effectiveness of free security solutions by country

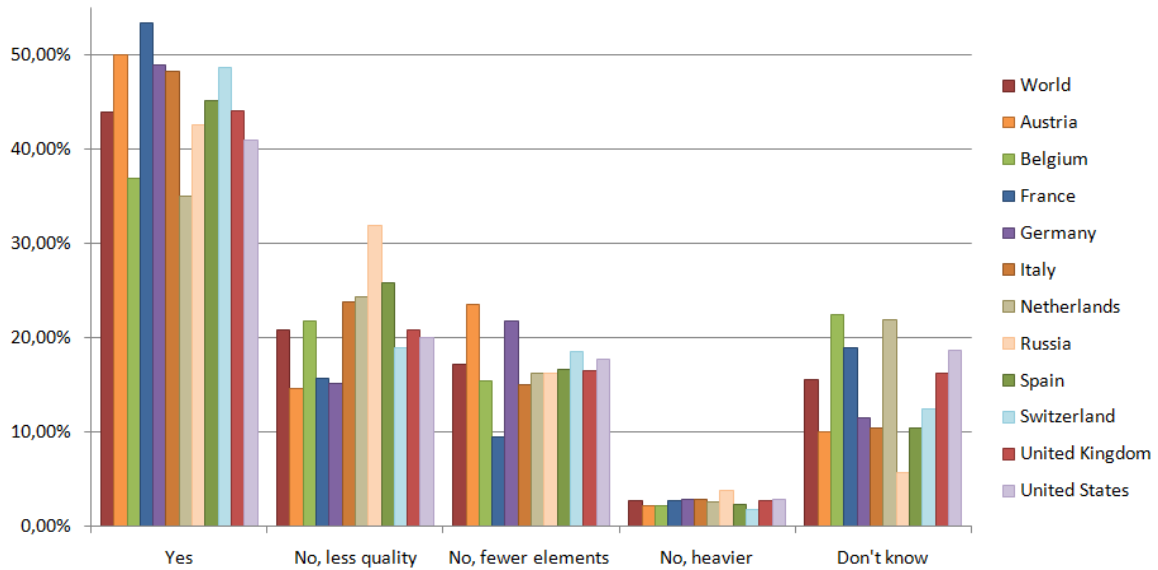


Table 6: Results of individual countries: is free security software as good as purchased security solutions in the respondents' opinion?

Is free security software as good as paid for software?					
	Yes	No, less	No, fewer elements	No, heavier	Don't know
World	43,94%	20,82%	17,08%	2,68%	15,48%
Austria	50,00%	14,58%	23,44%	2,08%	9,90%
Belgium	36,85%	21,77%	15,30%	2,16%	22,41%
France	53,32%	15,70%	9,47%	2,66%	18,85%
Germany	48,91%	15,08%	21,78%	2,85%	11,39%
Italy	48,15%	23,72%	14,94%	2,81%	10,37%
Netherlands	34,99%	24,32%	16,22%	2,56%	21,91%
Russia	42,58%	31,89%	16,22%	3,69%	5,62%
Spain	45,04%	25,74%	16,52%	2,26%	10,43%
Switzerland	48,60%	18,85%	18,41%	1,77%	12,37%
United Kingdom	44,03%	20,71%	16,46%	2,62%	16,18%
United States	40,94%	19,91%	17,68%	2,82%	18,65%

### 3.1.2 Number of unprotected PCs

There appears to be a general awareness among users of the need to secure one's personal computer. The number of unprotected PCs among survey participants was relatively low, at just 4 percent, or 659 of the users surveyed – so far so good. However, another 5 or so percent of users have no idea whether any security solution is installed on their system. Furthermore, 1.84 percent of respondents confessed to having installed pirated software. Therefore, on the whole, one can assume that around 6 percent of all survey respondents are using the Internet without any protection. Furthermore, it can be assumed that the respondents who did not know if they are using a security solution are also unprotected.

### Limited security awareness among Russian users

Compared to other countries, Russia has the most unprotected computers. The highest number of illegal versions of purchased security solutions is also installed here, with a share of almost 11 percent of users. Overall in Russia, 17 percent of PCs are inadequately protected against the threats lurking on the Internet. On the positive side, the leader is the United Kingdom, where just 6 percent of respondents gave answers leading to the conclusion that they are not shielded.

### 3.1.3 Suite protection or just virus protection?

Diagram 6: What security solution do users have installed?

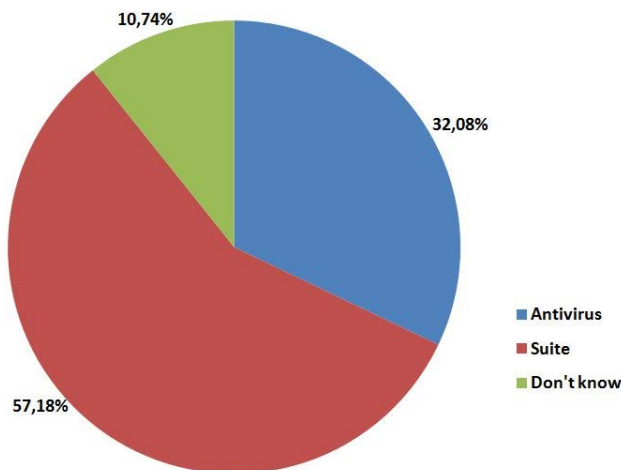


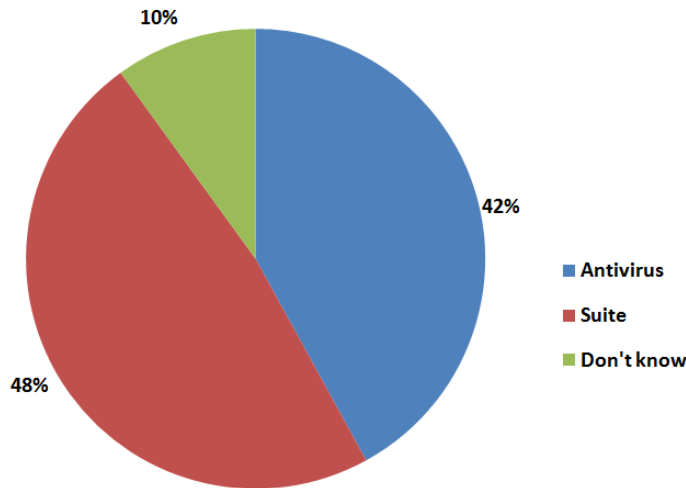
Table 7: Detailed results of the question on installed security solutions

What type of protection ?	Antivirus	Suite	Don't know
Men (18-24)	37,00%	55,29%	7,71%
Men (25-34)	35,52%	59,52%	4,95%
Men (35-44)	32,46%	60,69%	6,84%
Men (45-54)	29,55%	63,54%	6,91%
Men (55-64)	29,67%	62,93%	7,40%
<b>Total Men</b>	<b>32,73%</b>	<b>60,57%</b>	<b>6,69%</b>
Women (18-24)	36,03%	52,34%	11,64%
Women (25-34)	33,86%	53,39%	12,75%
Women (35-44)	29,92%	56,13%	13,95%
Women (45-54)	28,71%	56,29%	15,01%
Women (55-64)	29,23%	51,36%	19,41%
<b>Total Women</b>	<b>31,49%</b>	<b>54,05%</b>	<b>14,46%</b>
<b>Total</b>	<b>32,08%</b>	<b>57,18%</b>	<b>10,74%</b>

Internet users know that various threats lurk on the Internet and that they need to protect themselves against these threats. Or do they? If the results of the question asked previously (see diagram 2) are related to the question "What kind of security software do you have installed on your system?" there is an obvious contradiction: free security solutions consist exclusively of pure virus protection,

with no additional protection technology such as firewall, anti-spam or web protection. There are no free security packages on the market at present. Nevertheless, the majority of survey participants (see diagram 7) who had previously stated that they were using a free virus protection solution said that they were using an Internet security suite including a personal firewall, anti-spam and web protection.

Diagram 7: Installed security solution for users who said they were using a free security solution.



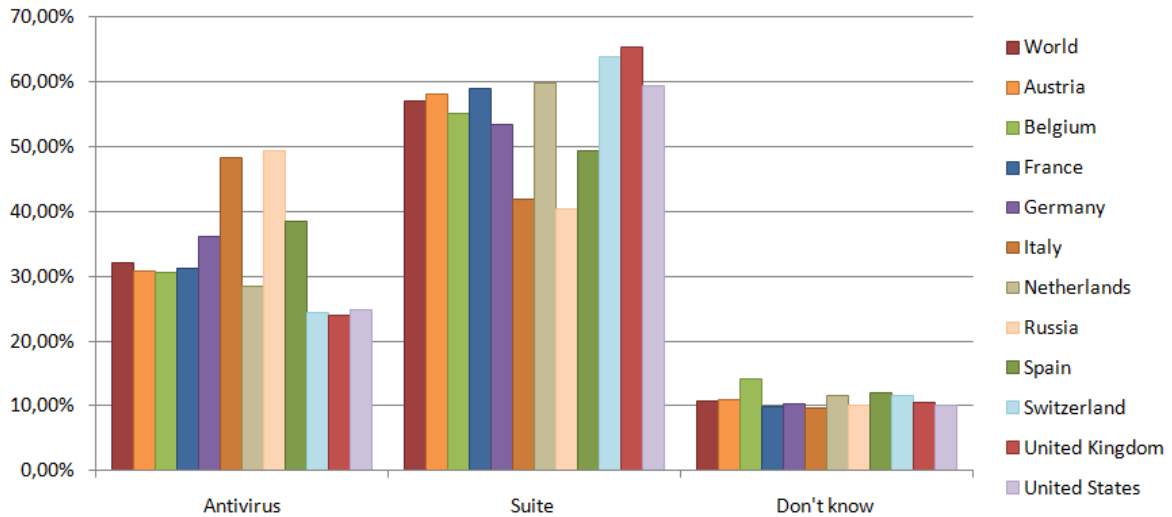
What does this apparent contradiction indicate? The majority of end users surveyed have the wrong impression of the features of mere antivirus programs compared to Internet security suites and appear to be inadequately informed about integrated protection technology. Therefore, the majority of users consider free antivirus and Internet security packages equivalent, regardless of the technological differences. This is a misunderstanding that can cost Internet users dearly, if one considers the various methods used to distribute malware.

Table 8: Installed security solutions in individual countries,

What type of protection?			
	Antivirus	Suite	Don't know
World	32,08%	57,18%	10,74%
Austria	30,86%	58,09%	11,05%
Belgium	30,70%	55,17%	14,13%
France	31,30%	58,90%	9,80%
Germany	36,17%	53,51%	10,32%
Italy	48,30%	41,92%	9,78%
Netherlands	28,55%	59,82%	11,63%
Russia	49,44%	40,45%	10,11%
Spain	38,52%	49,47%	12,01%
Switzerland	24,42%	63,92%	11,66%
United Kingdom	24,04%	65,33%	10,63%
United States	24,93%	59,35%	10,12%

However, in individual countries the number of users with a security package is larger than that of those using virus protection. The two exceptions to this are Italy and Russia, where the proportion is the other way around (see table 8).

Diagram 8: Installed security solutions by country

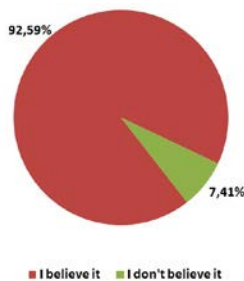


### 3.2 Where do web surfers expect there to be the most threats?

To get a picture of what Internet users are afraid of, with regard to online criminal activity, one thing G Data did was to suggest eleven false statements to the respondents. As it turned out, some respondents considered all of these false statements to be correct. Therefore, we are calling these statements the eleven assumptions of Internet security.

#### 3.2.1 The eleven assumptions of Internet security

##### Myth 1: When my PC is infected, I will notice in one way or another (93 percent).



This first assumption is the most widespread. Almost all Internet users (93 percent) around the world are convinced that malware has a distinct, identifiable effect on the PC. Accordingly, over 45 percent of all respondents assume that the computer will immediately crash in the event of a malware attack. Almost 57 percent are of the opinion that at least some functions will be disrupted or that specific software products will no longer work. 58 percent are convinced that the computer will display various pop-ups and emit distinct sounds if it is infected. Finally, almost 57 percent of respondents assume that the computer will run very slowly. Fewer than 7.5 percent are of the opinion that nothing noticeable will occur in the event of an infection, even though this is precisely what happens in the majority of cases (see table 9).

Table 9: What happens if a computer is infected, in the opinion of respondents? - Respondents were able to select multiple answers.

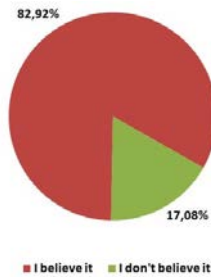
What happens when your PC is infected					
	PC crashes	Some things stop working	Strange pop-ups and sounds	PC becomes slow	Nothing special
Men (18-24)	43,52%	52,24%	56,64%	58,84%	10,45%
Men (25-34)	43,52%	57,46%	58,31%	59,96%	8,37%
Men (35-44)	46,35%	56,33%	58,58%	57,70%	7,99%
Men (45-54)	41,83%	54,57%	58,36%	57,03%	8,83%
Men (55-64)	37,44%	57,42%	54,89%	55,10%	7,10%
<b>Total Men</b>	<b>42,65%</b>	<b>55,71%</b>	<b>57,46%</b>	<b>57,77%</b>	<b>8,50%</b>
Women (18-24)	48,46%	58,18%	64,06%	62,52%	6,43%
Women (25-34)	50,17%	59,30%	64,37%	58,13%	5,57%
Women (35-44)	47,48%	57,51%	57,12%	55,27%	7,29%
Women (45-54)	46,81%	57,86%	56,22%	53,25%	5,65%
Women (55-64)	46,00%	57,23%	50,56%	48,17%	7,16%
<b>Total Women</b>	<b>47,85%</b>	<b>58,05%</b>	<b>58,62%</b>	<b>55,53%</b>	<b>6,40%</b>
<b>Total</b>	<b>45,35%</b>	<b>56,93%</b>	<b>58,06%</b>	<b>56,60%</b>	<b>7,41%</b>

In the past, malware was written by developers who wanted to show off their technical skills. If an infection occurred it was visible to the victim in the form of pop-ups, functional failures or because the computer would suddenly crash. Clearly people still remember such events well. Nowadays malware is programmed by professional and technically highly experienced criminals with the aim of earning as much money as possible. Well-programmed malware brings in a lot of money for the online black market. In this respect, program code is purchased from other criminals that can be used for setting up a botnet, for example, to enable access to the largest possible computing power using infected PCs all over the world. For example, these kinds of botnets enable so-called DDoS attacks to be carried out, spam to be sent or computer malware to be distributed. This aspect of the black economy has developed greatly: the developers and administrators of botnets offer their expertise and services as specialist service providers in special underground forums. Other criminals purchase services or malware on these platforms, e.g. to carry out an attack on a company website or launch a large spam distribution. No actual technical skill is required to do this.<sup>4</sup>

Therefore, the developers and administrators of botnets ensure that the botnet is as big and stable as possible. This means that every PC that gets disconnected (e.g. when the PC infection is discovered and removed) represents a financial loss for the cyber criminals. Malware is of course deliberately constructed by malware authors in such a way that the user cannot notice the infection. As a result, nowadays it is very unlikely that a PC infection is made visible by crashes, limited computing power, suspicious pop-ups or other characteristics. This development is very dangerous for PC users, because only an infection that occurs quickly can also be removed quickly. The situation is not exactly improved by the fact that nine out of ten users are still of the opinion that malware is easy to identify. Such users assume from the fact that their computer is running flawlessly that it cannot be infected. Therefore, this assumption plays right into the hands of cyber criminals.

<sup>4</sup> For further information on the underground economy, see the G Data Underground Economy White paper at: <http://www.gdatasoftware.com/information/security-labs/information/whitepaper.html>

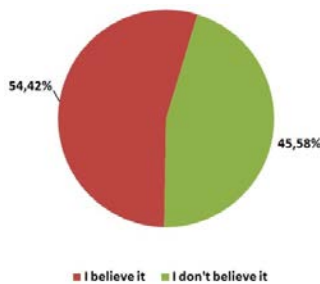
**Myth 2: Free AV software offers the same elements of security as paid for packages (83 percent).**



At 83 percent, the vast majority of respondents also support this false statement. When asked about the difference in quality between free and purchased security solutions (see table 6), even though the majority of respondents (56 percent) expressed doubt that the quality of both types of protective software is comparable, the majority of respondents cannot name the differences individually. 15 percent of respondents admitted having no idea how free security products differ from commercial solutions in terms of their capability. Almost 3 percent of respondents are of the opinion that the differ-

ence is in system load: the free products place a greater load on the system than purchased solutions. The major difference between free and purchased offerings is in what security technology they include. Free security software only provides basic virus protection. Purchased security software includes a range of security components: besides virus protection, the solutions generally include an HTTP filter, a firewall, an anti-spam module and behaviour-based recognition of malware. When asked this question, only 17 percent of recipients knew this.

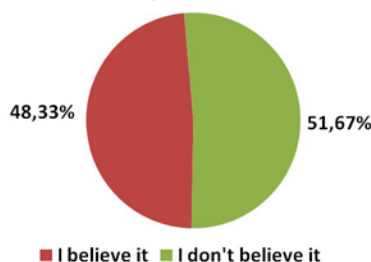
**Myth 3: Most malware is spread through e-mail (54 percent).**



This assumption is as out of date as the first, but even so 54 percent of respondents believe it. In fact, in the final years of the last millennium e-mail became by far the most frequently used distribution method for malware, with such spam as the "Melissa" and "I love you" e-mails. Infections are carried out via contaminated file attachments that have been talked up in the most interesting way possible via social engineering. Many people certainly remember the e-mails that promised naked photos of Russian tennis star Anna Kournikova. However, on opening this attachment a virus was actually installed on the PC. For the past six years or so file attachments in e-mails have been increasingly replaced by links to files on websites (even though file attachments have been booming again for several months) This tactic enables the perpetrators to bypass the highly effective spam filters with their e-mail and get it to unsuspecting users. On the other hand, many users have become very cautious when they receive e-mail from unknown senders and ideally delete them immediately without opening them first. These days, links in e-mails usually redirect to malicious websites. This also provides other options for finding victims, such as social networks (see section 3.3), optimising search terms, "typing-error domains", etc. The malware is moved to websites and websites have since become the number one point of infection.

**Myth 4: You can't get infected just by loading an infected website (48 percent).**

It is shocking that almost half of Internet users take this statement to be true. It has already been

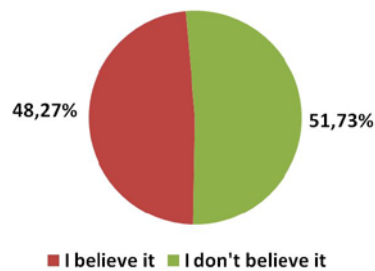


possible to use drive-by downloads to contaminate computers with malware for years now. All it takes to cause an infection like this is for someone to visit the website in question. Therefore, the assumption that downloading in itself is not enough has proven to be a dangerous fallacy, as this type of attack is carried out on a large-scale basis every day.

There are two types of drive-by infection: Firstly, there are websites that have been developed for the purpose of infecting PCs. The cyber criminals try to lure victims to

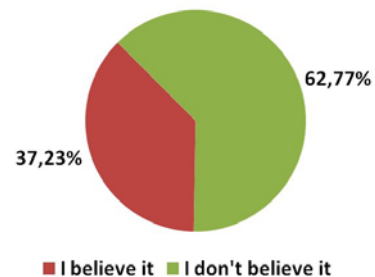
the infected website by publishing seemingly interesting links in social networks or by using banner adverts or e-mails containing the link. The other variant is more refined: malware code is smuggled onto a popular website that is actually trustworthy. For example, a window that is invisible to the Internet user of, say, 0 x 0 pixels is opened. However, it is used to launch a download whereby the visitor's PC is automatically and secretly infected with malware. The particular benefit for cyber criminals of this second method is that they do not need to do any advertising for the website. In order to achieve this, the perpetrators must penetrate the website to manipulate it accordingly. If it is well protected (which only applies to a small proportion of websites) this can be very difficult.

**Myth 5: Most malware is spread through downloads at peer2peer and torrent sites (48 percent).**



It is indisputable that a large volume of malware is distributed via swap platforms such as torrent websites and peer2peer networks. Therefore, it is not surprising that 48 percent of survey participants are of the opinion that this is the most important method for distributing malware. Users may have had their system infected with malware, following activity on such a site. Yet this assumption is also false and as such it is a myth, as the majority of malware is distributed via malicious websites (as already shown).

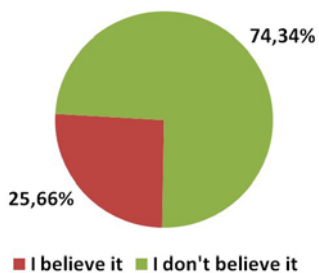
**Myth 6: It is more likely to encounter malware at a porn site than at a horseback riding site (37 percent).**



Pornography has a dubious reputation. Therefore, it is no wonder that many people (37 percent of respondents) assume there is a connection between pornography and Internet crime. However, it is questionable whether pornography sites are more frequently compromised than websites that address horse riding or other leisure subjects. The pornography industry earns a lot of money. The website represents the principal source of income for operators of pornographic websites. Accordingly, they are generally developed,

maintained and secured by professionals. A paying customer who picks up malware during their visit would be a lost customer for the operator and would represent a financial loss as a consequence. An amateur website operator is, perhaps, not a professional web designer and thus does not regularly install every new software update and patch required for closing security holes. Therefore, it is much easier for criminals to penetrate such websites and smuggle in malicious code than professionally developed pornographic websites. Furthermore, such websites are fairly easy to identify via Google: you just need to know the name of one of the applications and a security hole. A lot of websites that are easy to manipulate can be found in this way. But pornographic websites can harbour a higher risk overall if they exist for dubious reasons, although, on the other hand, the potential threat from serious sex sites is not so great.

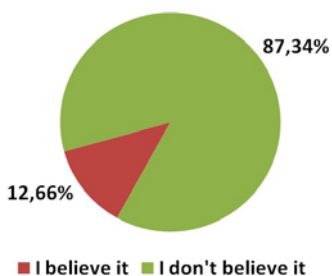
**Myth 7: My firewall can protect my PC from drive-by-download attacks (26 percent).**



sensitive data to criminals.

Some 26 percent of respondents believe this assertion. The assumption is wrong. Firewalls are certainly an important component of the protection plan for a computer. However, it is not possible to effectively protect a PC from drive-by infections using a firewall alone. Internet users are also recommended to use a comprehensive security solution with integrated web protection for effective, adequate security. Even with a successful infection, a firewall cannot always prevent the malware from running its malicious tasks and sending

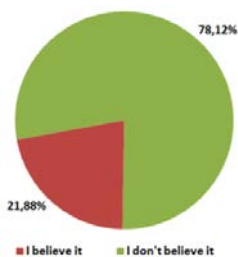
**Myth 8: I don't visit risky sites, so I am safe from drive-by-downloads (13 percent).**



this assumption.

This claim can be refuted in the same way as the sixth assumption ("It is more likely to encounter malware at a porn site that at a horseback riding site"). Cyber criminals pay no attention to the subject matter of a website. They are only interested in where they can infect the most visitors with malware for the smallest outlay. Criminals achieve this by, for example, manipulating web banners and constantly attacking large domains. If they are successful and gain access, they can use so-called web exploit toolkits to load malicious code without any specialist knowledge. Websites that have been highly trustworthy for years can suddenly be hacked in this way and so harbour a risk of infection. However, only some 13 percent of respondents believe

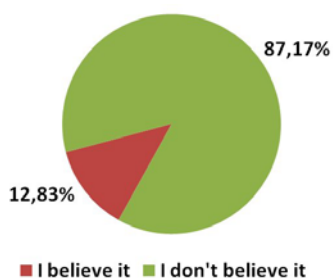
**Myth 9: If you don't open an infected file, you can't get infected (22 percent).**



does.

As with several other assertions made here, this claim is based on out-of-date facts and a lack of knowledge as almost 22 percent of survey participants believe the statement. Naturally, infections still occur when users open dangerous files. However, it is only possible for malicious files to be automatically executed if existing security holes are exploited by the attackers. In this case it might be possible for the malicious code to be activated automatically without clicking on the infected file. Therefore, you should always assume that infected files are dangerous for the PC user and can be executed regardless of what the user

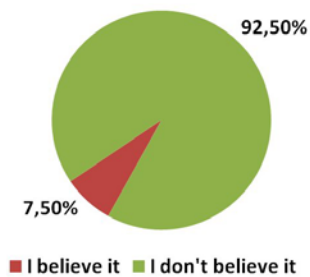
**Myth 10: Most malware is spread through USB sticks (13 percent).**



It has become evident that the majority of malware is distributed via malicious websites. However, other infection options are possible. In the eighties and nineties, when the Internet was not yet so universal, diskettes were still a frequent source of infection. In recent years the popularity of USB sticks and other external storage devices has significantly increased among cyber criminals. This allows the autostart functions in data media to be exploited for running malware programs

when connected to the PC. The most prominent example is the Conficker worm. Therefore, it is strongly recommended that the automatic run function in the operating system is disabled. This prevents worms from being installed when the USB stick is connected to the computer.

**Myth 11: Cyber criminals aren't interested in the PC's of consumers (8 percent)**



This assertion is given the least credibility of all as only 8 percent of respondents believe it to be true. Once again, it is a false assertion. Obviously corporate networks are of great interest to cyber criminals but in general, they are also harder to infect.

Even private computers are powerful today and are therefore ideally suitable as components in a botnet. Personal data such as access details for online shops, social networks and e-mail accounts or credit card information, is very often stored on them and is of great interest to cyber criminals. Therefore, the significance of private computers for cyber criminals should not be underestimated.

**3.2.2 Who is better informed: younger or older Internet users?**

As the research was exclusively carried out online, all respondents are active Internet users, yet the medium is relatively new for the more elderly of the respondents. Respondents in the age range between 18 and 25 have largely grown up with computers and are very active on the Internet. The situation with respondents in the age range of 55 to 64 is somewhat different. Therefore, it is understandable that the younger generation knows much more about risks on the Internet than the older generation.

However, another hypothesis suggests that the older generation is wary of danger due to the relative unfamiliarity with the Internet and computers, and therefore is much more cautious.

To establish the level of information among the youngest and oldest generation of respondents, we asked to what extent these two groups believe the assumptions given above. The following table provides an appropriate overview.

Table 10: Who believes the above assumptions more: younger or older users?

Myth	18-24 years group:	55-64 years group:	All of the responders:
1) When my PC is infected, I will notice in one way or another.	91,68%	92,87%	92,59%
2) Free FV software offer the same elements of security as paid for packages.	82,17%	83,17%	82,92%
3) Most malware is spread through e-mail.	46,54%	61,46%	54,42%
4) You can't get infected just by loading an infected website.	53,42%	46,67%	48,33%
5) Most malware is spread through downloads at peer2peer and torrent sites.	53,42%	45,67%	48,27%
6) It is more likely to encounter malware at a porn site than at a horseback riding site.	32,89%	17,47%	25,66%
7) My firewall can protect my PC from drive-by-download attacks.	39,18%	35,40%	37,23%
8) I don't visit risky sites, so I am safe from dive-by-downloads.	14,39%	13,69%	12,66%
9) If you don't open an infected file, you can't get infected.	22,42%	25,13%	21,88%
10) Most malware is spread trough USB drives	16,91%	9,02%	12,83%
11) Cyber criminals aren't interested in the PC's of consumers.	10,03%	6,77%	7,50%

When the column in the table for younger respondents is considered, the result is initially positive as this age group are less likely to believe the three biggest assumptions (although this only differs minimally from the average for all respondents.) However, the young respondents are much more inclined than other respondents to believe the fourth assumption, which is a very dangerous fallacy as it questions the existence and effectiveness of drive-by infections. This also applies to the fifth assumption concerning malware on swap sites such as torrent sites and peer2peer networks. The reason for this possibly lies in the fact that the younger generation downloads a lot of files from such sites and thus has already run into infected files. Younger respondents also imagine a somewhat higher risk with pornographic sites than older ones. The younger generation is clearly less informed of what functions a firewall has. This does not fit the hypothesis that younger users are more likely to understand technology and the internet. The younger generation is also less aware that it is not absolutely necessary to open a file for an infection to occur. Furthermore, the youngest respondents had an above-average belief that USB sticks are the most important source of malware infections. The younger participants over-estimate their knowledge of how they can prevent drive-by downloads more than older age groups. Furthermore, they assume far more than the average for respondents that their private computers are of no interest to cyber criminals.

On the whole, the younger respondents are not especially different. Their level of awareness is lower than that of the average Internet user, and therefore, the hypothesis that young people are more informed about the Internet than the average population is untenable.

If we turn our attention to the column for older respondents, it becomes clear that they are much more inclined to believe the three biggest assumptions than the average for respondents. With the fourth assumption, however, which concerns drive-by download attacks, the picture is different. Older respondents are clearly better informed about the risks of such attacks than respondents in

younger age ranges, and especially more so than the youngest users. However, even among the older respondents almost every other person believes that there is no such thing as a drive-by download. An above-average number of older survey participants are of the opinion that file sharing sites are the most important source of malware infections (although the difference from the average is small.) Pornographic websites are also met with less mistrust among older participants than the average. The older participants have much less trust in the protection functions of firewalls against drive-by downloads than the youngest and the average. On the other hand, older respondents are more likely to believe that it is impossible to be infected if a file is not opened, which actually contradicts the conviction of the risk of drive-by infections expressed before. Older respondents are less likely to see USB sticks as the greatest source of malware distribution but on the other hand, trust in the safety of their own surfing habits, which they think protects them against drive-by downloads. This could be because older people are still somewhat less carefree than younger users. One positive thing is that older respondents understand more than the average that their PCs can be of interest to cyber criminals.

All in all, older respondents are not well informed either, even though they clearly deal with threats on the Internet better than the youngest respondents. This analysis leads to the conclusion that the 25-54 age group can boast the best awareness of the threats on the Internet. However, it must be pointed out that numerous false assumptions on this subject are circulated in this age group as well, and that the level of knowledge among these respondents is not perfect.

### 3.2.3 In which country are Internet users best informed of the risks?

There are many preconceptions about which countries' users are better or worse informed. For example many people assume that Americans and Britons are well-informed of threats on the Internet, but that Italians and Russians are somewhat less well informed. To find out whether there actually are countries where Internet users are much better or worse informed of the actual threats on the Internet, the percentage results of respondents who believe in the above myths are set out in table 11. Green indicates the countries in which the assumption is believed the least. Red indicates where the assumption gets the most support.

Table 11: In which countries are the assumptions believed the most?

Myth	Netherlands	Belgium	France	Spain	United States of America	Italy	Germany	Russia	United Kingdom	Austria	Switzerland	World
1) Apparent infection	86,63%	93,97%	92,28%	95,30%	94,29%	94,38%	83,17%	97,88%	91,40%	86,46%	90,13%	92,59%
2) Free AV	83,78%	83,19%	90,53%	83,48%	82,32%	85,06%	78,22%	83,78%	83,54%	76,56%	81,59%	82,92%
3) Infected e-mail	58,89%	62,18%	57,64%	58,61%	52,37%	58,88%	52,85%	38,80%	52,89%	55,47%	57,73%	54,42%
4) Infected website	51,49%	49,03%	49,25%	57,83%	40,95%	63,44%	62,90%	48,48%	42,85%	60,68%	54,93%	48,33%
5) Torrent and peer2peer	43,53%	46,76%	48,17%	52,43%	52,73%	45,52%	35,26%	49,49%	48,73%	41,02%	44,48%	48,27%
6) Infected porn site	25,32%	34,27%	31,89%	32,43%	40,13%	32,25%	30,65%	60,18%	35,80%	34,11%	36,23%	37,23%
7) Firewall	31,44%	28,34%	18,77%	26,78%	24,32%	28,03%	29,31%	17,05%	24,95%	28,26%	29,16%	25,66%
8) Risky sites	18,07%	13,69%	14,78%	14,00%	10,79%	17,84%	11,81%	11,89%	9,67%	12,50%	14,14%	12,66%
9) Infected file	16,50%	26,29%	23,59%	30,78%	18,18%	30,67%	13,32%	38,53%	20,43%	14,06%	18,56%	21,88%
10) Infected USB-stick	8,11%	10,67%	17,28%	20,09%	9,92%	15,38%	8,38%	30,05%	10,49%	8,72%	8,98%	12,83%
11) Private PC's	5,12%	6,90%	5,98%	8,87%	7,50%	8,35%	7,20%	6,54%	8,77%	9,90%	6,63%	7,50%

This table shows that respondents from Germany are clearly the best informed of the threats lurking on the Internet. They believe three of the assumptions the least of all countries. Although the same applies to the Dutch, it should be noted that the Dutch are furthest from the truth in assessing the assertions on two occasions. Interestingly, the Americans (among whom the clearest distinction might perhaps have been expected) only exhibit the lowest number of advocates for the fourth assumption. American respondents most believe the assumption that the majority of malware code is distributed via swap sites. Yet it is not the Americans who are worst informed of threats on the Internet: Russia comes in last. The Russians believe four of the false assertions the most out of all the nationalities. Although they believe two of the other myths the least, this does not keep them from last place in the ranking.

### 3.2.4 Are men the better surfers?

There is an assumption in society that men are more technically adept than women and therefore better informed on Internet threats. But is this really the case? The following table shows the results of Internet myths in relation to gender.

Table 12: Who believes the assumptions more: men or women?

Myth	Men	Women	Total
1) When my PC is infected, I will notice in one way or another.	91,50%	93,60%	92,59%
2) Free AV software offer the same elements of security as paid for packages.	84,01%	81,73%	82,92%
3) Most malware is spread through e-mail.	54,53%	54,31%	54,42%
4) You can't get infected just by loading an infected website.	48,19%	48,46%	48,33%
5) Most malware is spread through downloads at peer2peer and torrent sites.	49,13%	47,47%	48,27%
6) It is more likely to encounter malware at a porn site than at a horseback riding	43,88%	31,07%	37,23%
7) My firewall can protect my PC from drive-by-download attacks.	26,02%	25,32%	25,66%
8) I don't visit risky sites, so I am safe from drive-by-downloads.	11,74%	13,51%	12,66%
9) If you don't open an infected file, you can't get infected.	22,65%	21,16%	21,88%
10) Most malware is spread through USB drives.	13,47%	12,24%	12,83%
11) Cyber criminals aren't interested in the PC's of consumers.	8,75%	6,35%	7,50%

The table shows that women are significantly closer to the truth than men as women are only wrong more often than men with three of the false statements. Yet whether this alone can lead to the conclusion that women are better Internet users is questionable as in most cases the resulting percentages are separated by less than 2 percent.

The clearest difference between men and women appears in the assumption "The risk of encountering malware is greater on pornographic websites than for example when visiting horse riding or travel websites". 43.88 percent of men believed this as appose to just 31.07 percent of women. A possible reason for this can be explained in the same way as the answers from younger respondents, who believe the following statement the most: "The majority of viruses and computer malware is distributed via infected files in swap shops such as peer2peer networks and torrent websites". The more a target group visit such websites, the more likely they are to have been afflicted with malware.

Another statement which shows a difference between men and women is in the myth 'Cyber criminals aren't interested in the PCs of consumers.' Men are more likely to believe the statement which could suggest that women are generally more cautious with their PCs.

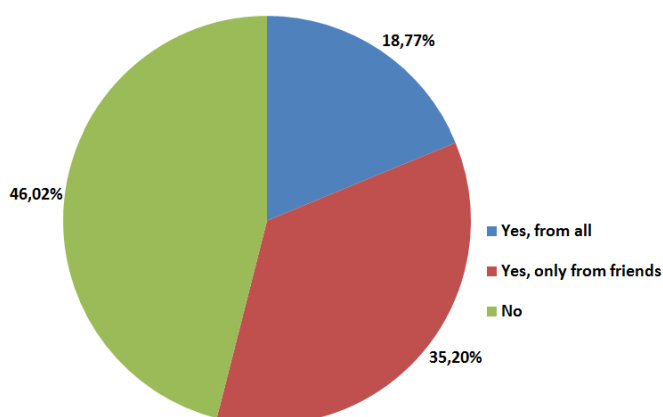
### 3.3 Behaviour on social networks

Social networks are becoming more and more popular and have thus become a fixed component of the Internet landscape. However, the huge popularity of social networks is increasingly bringing criminals onto the scene, abusing social portals for their criminal activity.

The fraudsters have numerous options for harming users: Essentially, they can use "standard" phishing techniques to steal users' network access data with the aid of deceptively real looking websites, or to steal data from the provider's access database. One very common criminal scam on social platforms is the distribution of malicious web addresses via wall postings, chat room messages or personal messages. This scam is often related to video content.

The websites users are lead to, are often so heavily shortened by a URL shortening service that the user is unaware there is any risk. Clicking on the link takes them to an external website that is either contaminated with malicious code, uses phishing to steal data or uses clickjacking to make the victim a spam 'spray-gun' on the social network. That way, the user unwittingly forwards the link to his network of friends, without being able to see what is happening. Therefore, caution is advised when receiving links from people you do not know; however, friends can also distribute such web addresses, e.g. if their user account has been hacked and exploited by a criminal. Because of the high risk potential, the G Data 2011 Security Survey included the question of whether users click on links in social networks.

Diagram 9: Click behaviour for website URLs in social networks.

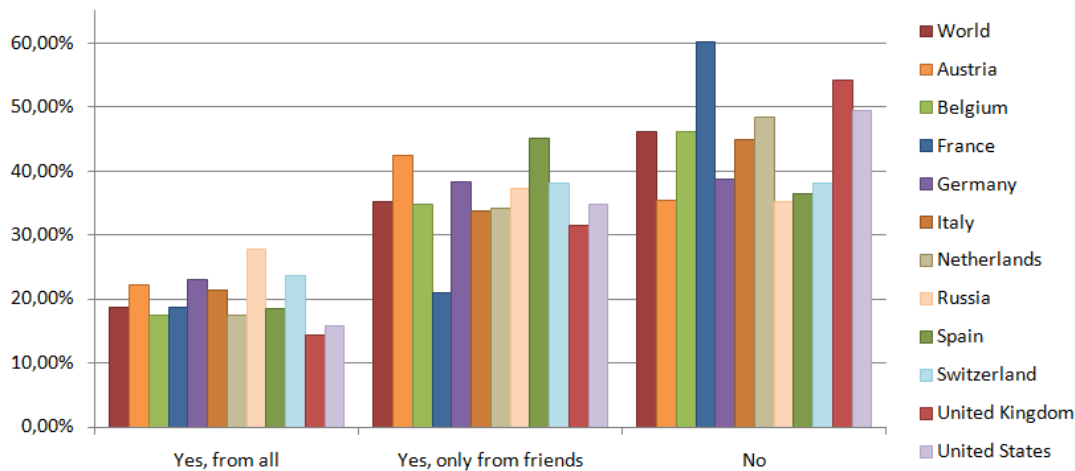


The majority of participants in the survey do not use links offered in social networks, regardless of whether they originate from friends or people they do not know. Over a third trust the web addresses that friends in their own network have published and only 19 percent click on links regardless of from whom they came, thus making themselves easy targets for cyber criminals and their illegal activities.

**France is especially prominent in the comparison of countries:**

60 percent of French respondents do not click on links in social network, this is the highest value compared to all the other countries. 18 percent of the French participants claimed they click on website links in social networks from any user. This value is exactly the same as the average value in the comparison of countries. Furthermore, just 21 percent of French respondents click on website links that members of their network of friends have posted on social platforms. Compared to other countries and the average value, this is the lowest figure. Accordingly the French appear the most sensitive to the risks of linking to websites in social networks.

Diagram 10: Click behaviour for website URLs in social networks by country



Respondents from Russia are the least aware of the dangers of links on social networks: over a quarter of respondents say that they click on URLs from any known or unknown social network user. Only 35 percent do not click on any website URLs. 37 percent of Russian respondents only click on web addresses from friends.

Table 13: Click behaviour for website URLs in social networks by individual country

Do you click on links in social networks?			
	Yes, from all	Yes, only from friends	No
World	18,77%	35,20%	46,02%
Austria	22,27%	42,45%	35,29%
Belgium	17,34%	34,80%	46,17%
France	18,77%	21,01%	60,22%
Germany	22,95%	38,36%	38,69%
Italy	21,44%	33,66%	44,90%
Netherlands	17,50%	34,14%	49,36%
Russia	27,74%	37,14%	35,12%
Spain	18,43%	45,04%	36,52%
Switzerland	23,71%	38,14%	38,14%
United Kingdom	14,29%	31,46%	54,25%
United States	15,79%	34,80%	49,41%

### 3.3.1 Who behaves more safely in social networks: men or women?

The results from the G Data Security Survey show a difference between men and women in terms of usage of links in social networks. However, the difference is fairly small: 47 percent of women avoid links in social networks, whereas men are slightly lower at just 45 percent.

In contrast, men are more likely to click on links that do not come from members of their network of friends. Women are more than twice as likely to click on URLs from friends as from someone they do not know. Around one third of male respondents only click on web addresses from friends.

Table 14: Detailed results for the question (total result for all countries)

Do you click on links on social networks?			
	Yes, from all	Yes, only from friends	No
Men (18-24)	26,24%	38,02%	35,74%
Men (25-34)	25,92%	38,63%	35,45%
Men (35-44)	21,09%	33,56%	45,35%
Men (45-54)	18,23%	31,10%	50,66%
Men (55-64)	15,93%	26,21%	57,86%
<b>Total Men</b>	<b>21,46%</b>	<b>33,55%</b>	<b>44,99%</b>
Women (18-24)	21,54%	45,38%	33,08%
Women (25-34)	20,43%	40,92%	38,64%
Women (35-44)	15,41%	35,59%	48,99%
Women (45-54)	13,72%	31,27%	55,01%
Women (55-64)	9,83%	30,48%	59,69%
<b>Total Women</b>	<b>16,29%</b>	<b>36,73%</b>	<b>46,99%</b>
<b>Total</b>	<b>18,77%</b>	<b>35,20%</b>	<b>46,02%</b>

With the exception of Italy, Belgium and Austria, the results in individual countries provide a similar picture, that women are essentially more cautious in social networks than men as on the whole, women avoid clicking on URLs in social networks. However, the results of the G Data Security Survey show opposite results in Italy, Belgium and Austria. In these countries, men seem more sensitive to risks from links on social platforms, although the difference here is minimal.

The results show that there are differences between men and women, but overall they are very small. Therefore, it is not easy to draw the conclusion that one of the two genders is more cautious in using social networks.

### 3.3.2 Who behaves more safely in social networks: younger or older users?

Younger Internet users are stereotypically more frequent on social networks than older surfers. Nevertheless, the G Data Security Survey indicates that the older generation is more cautious in the use of social platforms. Especially cautious are men and women in equal measure in the two older age groups, 45-54 and 55-64 (see table 14) as more than half of these respondents do not click on URLs in social networks. In contrast, the three younger age groups (up to 44) are much more likely to click on posted web links on social networks.



### **Conclusion: the "silver surfer" generation is slightly ahead**

The older the respondents are, the less likely they are to click on links to external websites in social networks. Therefore, it is irrelevant whether they come from people they do or do not know. Whereas almost 58 percent of men from 55 to 64 will not click on links, just 36 percent of men in the 18 to 24 age range refuse to do so. The difference is even bigger with women: in the oldest age range 60 percent refuse to click on links, as opposed to just a third of women from 18 to 24. This indicates that the younger the female respondent is, the more she is to click on links in social networks.

The caution that older users show can have a number of origins. Firstly, the older generation is generally less familiar with social networks; therefore, there is a fundamental uncertainty among some older people in their use of social portals. Also, older people do not use social networks with the intensity that young users do (e.g. via mobile devices) and generally, do not spend as much time on them. Furthermore, there is the possibility that the contacts in these older age groups' networks are less likely to publish external links and so the respondents do not come into contact with this issue as often as younger users.

## 4. Conclusions

The research allows one very positive conclusion to be drawn: the majority of Internet users, regardless of age, sex or nationality, are aware that there are threats on the Internet.

Unfortunately with most users, this awareness is somewhat out of date, as only a small percentage of respondents can give correct answers for current threats on the Internet. Knowledge of how users can effectively protect themselves against computer malware is also quite limited among respondents.

Furthermore, it turns out that there are many misleading assumptions circulating about threats on the Internet. Almost everyone thinks they know what to do with viruses and other malicious codes, but rely on very out-of-date facts in doing so. There is a great deal of concern about threats that only occur rarely today, such as malware that is mass-distributed via e-mail (54 percent think that the majority of computer malware is distributed this way), or the assumption that malware will affect the PC in some way (92 percent think this). Although this was still the case in the nineties and to an extent in the first decade of the new millennium as well, this has not been true for some time now. These days the majority of malware is so skilfully programmed that it is almost invisible to PC users, one of the exceptions being fake security programs called rogeware. Therefore, there is rarely a problem, with regard to the misguided belief that the majority of malware is sent via e-mail. With that said, it is always advisable to exercise caution when dealing with e-mail. Clicking on links and opening attachments continues to harbour risks. A high level of awareness here can surely do no harm.

The other assumption, that computer malware cripples the computer, creates more trouble. The misguided assumption that as long as the user cannot detect any problems on his computer, he thinks himself safe is also problematic. As previously stated, malware infections today are not visible to users. Therefore, the malware is capable of fulfilling its purpose for a long time and the perpetrators profit from its results.

Another sobering insight is the fact that the threats coming from websites are relatively unrecognised. Almost half of respondents do not believe that drive-by downloads exist. 48 percent of survey participants do not think that you can infect your computer just by visiting a contaminated website. This method of infection is currently the one most commonly used by cyber criminals to distribute malware. Those users that have heard of drive-by infections or know of them often have distinct notions of where they will mostly find infected websites of this sort. Men especially (almost 44 percent) think that pornographic websites carry an above-average level of danger. However, this also implies that infected websites are not randomly dispersed across the entire web. Moreover, this assumption does not take into account that known, trustworthy websites can be hacked and infected with malicious code. Almost every week there are reports in the media regarding major consumer brands whose websites have been hacked. And those are just the cases that make it into the media. Who knows how many cases remain undiscovered? In short: drive-by infections, as the name suggests, cannot be foreseen by users. Consequently, it is not possible to use your behaviour alone to prevent the PC from coming into contact with these at some point.

The only effective way to protect PCs from drive-by downloads is to use a comprehensive security solution that contains an HTTP filter that scans websites for malware before they are loaded. Free antivirus solutions do not contain such protection technology, so users are not properly protected. Instead, users are often of the opinion that the solution they have installed provides the necessary, comprehensive protection against threats on the Internet, as the survey has indicated. This misconception could be disastrous and lead to infection with dangerous malware.



No less than 62.58 percent of users of free antivirus solutions believe that the product will protect the PC from drive-by downloads. A total of 25.39 percent of users incorrectly assume that their PC will be protected from drive-by downloads by their firewall. This incorrect assumptions means users will not be on the lookout for an HTTP filter to protect themselves against infected websites.

Protection against infected websites is also very important for social network users. Links to external websites containing humorous or informative content, or film clips are constantly being published on such platforms. These functions make networks such as Twitter and Facebook attractive to users. Therefore, it would be a mistake to ignore such links for security reasons, although that is precisely what 46 percent of participants in the survey are doing. In this regard, it must also be said that shortened website URLs represent a heightened risk, and not just on social platforms. The target of a shortened link is not immediately recognisable. Online services such as <http://longurl.org> can be used to determine the original e-mail address. Such services used in conjunction with a good HTTP filter make it slightly safer for users to click on links published on social networks.

Conclusions as to who is best informed regarding threats overall are hard to draw. Clearly the middle and high-end age groups of respondents from 25 to 54 are best informed of the threats on the Internet, but they often also have misgivings over situations that harbour almost no threats. Whether they can be considered as more prudent users of the Internet is therefore doubtful.

The difference between men and women turns out to be very small, even though women appear to be slightly better informed in the overall results of the G Data 2011 Security Survey. Therefore, it is not possible to draw a general conclusion as to which of the two sexes is more aware of the potential threat on the Internet. Even when the nationality of the respondents is taken into account, it is impossible to determine a clear winner.

Users in Germany and the United Kingdom are clearly better informed as to which Internet threats are real and which are not, but even in those countries the differences to the overall average are only minimal.

However, one result is significant: the greatest lack of awareness of threats on the Internet is in Russia. Luckily, on the other hand, the proportion of Russian surfers who use purchased security suites is the highest by country. However, it should be noted that the largest number of pirate copies of purchased security suites is used in Russia, these being less stable and less reliable than the legal versions.

As a final conclusion to the G Data 2011 Security Survey, it should be said that despite the very widespread use of the Internet, the majority of users know little of the threats and thus have hardly any awareness of the strategies used to prevent computers from becoming infected with malware.



## Appendix

### G Data Software AG

G Data Software AG, based in Bochum, is an innovative and quickly expanding software house focusing on IT security solutions. A specialist in Internet security and pioneer in the field of virus protection, the company, which was founded in Bochum in 1985, developed the first antivirus program more than 20 years ago.

Consequently G Data is one of the oldest security software companies in the world. Over more than five years, no other European security software provider has won national and international tests and awards more frequently than G Data.

The product range consists of security solutions for end customers as well as medium to large-sized enterprises. G Data security solutions are available worldwide in more than 90 countries.

More information about the company and the G Data security solutions is available at [www.gdatasoftware.com](http://www.gdatasoftware.com)

#### **G Data milestones**

##### **1986**

CeBIT is born and G Data presents its first virus protection concept for the ATARI computer at the launch of the trade fair.

##### **1987**

G Data develops numerous innovative programs for the ATARI ST, including the world's first virus protection program, the G Data AntiVirusKit.

##### **1990**

The growth in personal computer use races ahead. G Data starts developing software for MS-DOS. The first project is converting the AntiVirusKit for PCs - with a novelty for the time: its own graphic user interface.

##### **1991**

G Data is continuously growing and offers a wide spectrum of different software programs for ATARI ST.

##### **1992**

Alongside virus protection programs, G Data develops numerous application software packages for MS-DOS and Windows. One particular innovation was the GeoRoute route planner - the first PC route planner with an interactive map.

##### **1995**

The first foreign subsidiary is opened in Poland.

##### **1998**

With over 1 million units sold, PowerRoute has become the most successful PC route planner in Germany

##### **2000**

Becomes a public company: G Data employees become company shareholders. Today, the majority share stake still belongs to employees and company founders.



**2001**

Enters the network and business market with G Data AntiVirus Business and AntiVirus Enterprise.

**2002**

G Data develops DoubleScan technology and becomes the first producer to use two virus engines in parallel within its products.

**2003**

Going International: market début in Japan

**2004**

G Data presents the first generation of its comprehensive security software package, G Data InternetSecurity, at CeBIT.

**2005**

Ahead of its time: G Data is the first company in the world to integrate cloud security technology in its range of protection programs. OutbreakShield provides real-time protection against spam and unknown computer malware, regardless of content.

The Stiftung Warentest (German consumer group award) nominates G Data InternetSecurity as best security package.

Going International: opening of subsidiaries in France and Italy

**2006**

The number of computer malware programs increases - G Data responds: hourly signature updates ensure that G Data customers are quickly protected against new malware.

**2007**

Stiftung Warentest: for the second time in a row G Data InternetSecurity 2010 wins first place in the famous consumer magazine's large benchmarking test.

CeBit launch 2007: G Data TotalCare

**2008**

Market début of a security solution specifically for notebook users: G Data NotebookSecurity is a powerful all-in-one solution that combines virus protection, backup and encryption technology.

**2009**

G Data security solutions are available worldwide in more than 60 countries. With market entries in South America, Russia, South Africa and China, G Data continues its successful expansion policy.

**2010**

G Data celebrates its 25th Company Anniversary

CeBIT launch: G Data EndpointProtection

**2011**

CeBIT launch: G Data CloudSecurity - free browser plug-in for secure Internet surfing, smarter protection for Android smartphones and tablet PCs: G Data MobileSecurity



## Survey Sampling International

SSI established its commercial sampling business in the USA in 1977. We have been setting the standard for expert knowledge and the quality of sampling and customer service in the market research sector for over three decades.

SSI provides access to over 6 million survey participants in 54 countries. Our sources include our own SSI panel communities in 27 countries, a growing number of subsidiary companies operated by us and our comprehensive global network of partner companies. SSI has 400 employees in 50 countries, speaking 36 languages and it works on behalf of over 1,800 market research customers and three quarters of the world's largest market research companies.

The company has over 17 sites around the world: Peking, Frankfurt, London, Los Angeles, Madrid, Mexico City, Paris, Rotterdam, Seoul, Shanghai, Shelton (CT), Singapore, Stockholm, Sydney, Timisoara (Romania) Tokyo and Toronto. There are also SSI representatives in Hong Kong.

For more information on Survey Sampling International, please visit [www.surveysampling.com](http://www.surveysampling.com)

## Glossary

**Bot:** Bots are small programs that generally run unnoticed in the background on the victim's computer. Depending on the range of functions, they then carry out various tasks, from DDoS attacks to spam e-mail, recording keystrokes and much more. The range of functions essentially depends on how much someone wants to spend on a bot. Naturally bots with a very large range of functions are more expensive than somewhat simpler bots that can do very little. For example, they can be purchased in underground forums.

**Botnets:** A botnet is a network of so-called zombie PCs. Command and Control Servers (C&C Servers) are used to administer the botnet. Amongst other things, botnets are used to launch overload attacks on web servers (DoS and DDoS attacks) and to send spam.

**DoS (Denial of Service):** During a denial of service attack, computers (usually web servers) are flooded with targeted and/or vast numbers of queries. As a result, they are no longer able to function and crash under the load.

**DDoS (Distributed Denial of Service):** a Distributed Denial of Service attack is based on the same principle as a normal DoS attack, the difference being that this involves a distributed attack. Such attacks are often carried out using many thousands of zombie PCs.

**Drive-by-Infection (Drive-by-Download):** In a drive-by infection, malware is silently downloaded and executed on the computer when a primed website is visited. The perpetrators of such attacks exploit security holes in the browser and its plug-ins. Attackers pay particular attention to vulnerabilities in functions for executing active content (e.g. JavaScript, Flash or Java).

**Exploit:** A program that exploits an existing vulnerability on the target computer, in order to execute any program code.

**Phishing:** Phishing means an attempt to obtain personal data such as login names, passwords, credit card numbers, bank account login data, etc. via bogus websites or unsolicited e-mail. Phishing attempts often target bank customers with online banking offers (Citibank, Postbank), payment ser-



vices (PayPal), Internet service providers (AOL) or online shops (eBay, Amazon). People are often directed to counterfeit websites that are made to look just like the model sites via e-mail or Instant Messenger.

**Social engineering:** Social engineering refers to the persuasion tactics used by hackers to get Internet users to divulge information which they can then use to cause damage to these Internet users or their organisations. This often involves faking a role of authority, in order to gain access to data or passwords.

**Spam:** In the mid-1990s spam became the term used to describe the inordinate dissemination of the same message in Usenet forums. The term itself comes from a sketch by Monty Python. Nowadays, spam has several meanings. As a generic term, spam stands for sending any unsolicited e-mail. In a narrower sense, the term 'spam' is limited to advertising e-mails, meaning that worms, hoaxes, phishing e-mails and autoresponders are not included in this.

**Zombie PC:** A zombie PC is one that can be remotely controlled through a backdoor. Just like the model in films, the zombie PC only obeys its hidden master and executes his (usually criminal) commands. Usually, a number of zombies are combined into 'botnets'.