EISAS Basic Toolset 1.0

Feasibility Study of Home Users' IT Security

enisa
European Network and Information Security Agency

Credits

This study was commissioned by ENISA to the Ludwig-Maximilians-Universität München in Munich, Germany (LMU Munich, http://www.lmu.de/). The editor wishes to thank the author of the study, Dr Werner Degenhardt, LMU Munich, and co-researcher Mr Klaus Tingholm Kristensen, i-Trust, for their work. The researchers wish to express their gratitude to the participating organisations for their great support in conducting this study, especially Dr Ernst Bötsch of Leibniz-Rechenzentrum (http://www.lrz.de) and Mr Joachim Wolff of Versicherungskammer Bayern (http://www.vkb.de) for their extensive support.

About ENISA

The European Network and Information Security Agency (ENISA) is an EU agency created to advance the functioning of the internal market. ENISA is a centre of excellence for the European Member States and European institutions in network and information security, giving advice and recommendations and acting as a switchboard of information for good practices. Moreover, the agency facilitates contacts between the European institutions, the Member States and private business and industry actors.

Contact details

The study was edited by Mr Kjell Kalmelid, Expert, ENISA. For questions related to this study, EISAS or for general enquiries on CERT cooperation, please use the following contact details:

E-mail: CERT-Relations@enisa.europa.eu

Internet: http://www.enisa.europa.eu/act/cert/

Table of Contents

1 Executive summary

This study is part of the activities taken under the European Information Sharing and Alert System (EISAS) framework and looks into the problem of information technology (IT) security awareness programmes and IT security education of citizens at home. Citizens and small and medium enterprises (SMEs), constitute the largest group of Internet users in the European Union. IT systems owned and operated by those users are more exposed to the risk of becoming infected by malware and, in particular, of becoming part of a botnet – a network of compromised computers under malicious remote control.

The reason is that the computers of those end-users are generally less protected than those in large organisations and companies. Among other things, botnets are used for initiating DDoS attacks against organisations. Without proper security behaviour, citizens' home computers will indirectly and unknowingly pose a threat to the functional and sound Critical Information Infrastructure when performing everyday tasks on IT devices connected to the Internet.

In this context the general goal of EISAS is to:

- empower all EU citizens and SMEs with the knowledge and skills necessary to protect their IT systems and information assets;
- build on national capabilities of EU Member States;
- enhance cooperation between national/governmental CERTs in the EU Member States.

With regards to empowering citizens and SMEs, the first obstacle is that there is just too much information available that is not tailored to the problem context of the user. The second obstacle is that home users are not easily reached by IT security information.

These shortcomings need to be addressed once and for all.

The main objective of this feasibility study has been to develop and validate a 'ready-to-use' information security awareness-raising concept ('EISAS Basic Toolset'). The EISAS Basic Toolset will be a set of methodologies and tools that facilitates outreach to different sub-categories of the EISAS target groups with information about IT security in order to efficiently empower them with the necessary means and skills to protect their computers. The study acknowledges that there is a long road to travel from knowledge to behaviour. The outcome of the study 'EISAS Basic Toolset' shows that approaching the home user via his/her role as an employee of an organisation or enterprise works

well. The key success factors of enhancing the reach and outreach of IT security education measures for home users are listed below.

- Address employees in their role as home users directly by e-mail or other means of personal contact by a trusted person or entity of the organisation. Just putting a link on a website does not work.
- Provide information and tools tailored to the understanding and skills of the target groups. A one-size-fits-all approach will not work.
- Provide the opportunity for feedback and comments.
- Acknowledge the fact that the most important source of help to the user is a personal network of technically competent individuals.
- Bring the fact that there is help right in front of the eyes of the users, for example, by introducing a 112-Internet emergency button for the browser that connects the home user to his/her preferred information sources and trusted specialists.

2 Background

Citizens and small and medium enterprises (SMEs) constitute the largest group of Internet users in the EU. IT systems owned and operated by these users are popular targets for hackers to, for instance, steal valuable personal information such as credit card numbers or customers' details or to be incorporated into botnets, i.e. networks of remotely controlled computers. A botnet, in turn, is the means used to massively distribute spam and malware or to carry out Distributed Denial of Service attacks ('DDoS attacks') against networks.

A successfully conducted DDoS attack will inevitably cause damage for the targeted organisation by causing longer or shorter disruptions of communication services and information systems. In the worst case, the networks and systems attacked would be part of Critical Information Infrastructures (CIIs), which makes DDoS attack a serious threat to society at large.

The reason that computers of citizens and SMEs are being targeted by hackers is because the computers of those end-users are generally less protected than those in large organisations and companies. In general, large organisations have more resources at their disposal for managing information security risks, including having experts in charge of ensuring the appropriate protection of the organisation's computers, and are able to invest in carrying out awareness-raising activities and provide training for their employees, i.e. end-users.

That is, without proper security behaviour citizens at home will pose a threat to the functional and sound Critical Information Infrastructure when performing everyday on IT devices connected to the Internet.

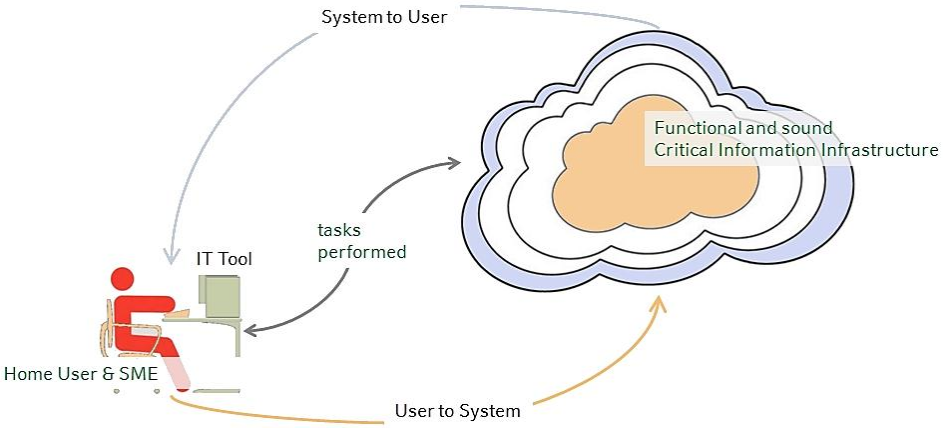


Figure 1 Interaction of system and user from the IT security perspective

Until now the response of society to citizens' lack of expertise in network and information security, lack of awareness of threats and risks to their computers, and lack of knowledge about how to protect themselves against those risks and threats has been the focus of awareness-raising initiatives.

In fact, the EISAS feasibility study shows that there is a great deal of good quality information available on the national Computer Emergency Response Team (CERT) websites and other initiatives that could be accessed and used by citizens and SMEs to advance security at home and at the SME workplace.

The FISHA project[1] can be seen as building on EISAS and shows that there are ways to enhance the cooperation amongst the national information-providing bodies and organisations. The project has started to address the EISAS activities of information collection, information processing (consolidation and formatting) and information dissemination (making information available) as part of transmitting security information from the source to the end-user chain.

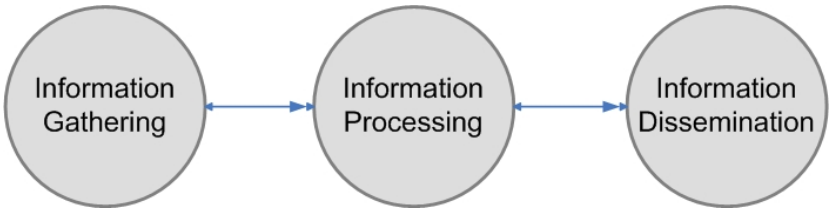


Figure 2 EISAS activities

There is, however, still more to be accomplished with regards to the European Commission's goal to 'empower all EU citizens and SMEs (seen similar to end-users in their security behaviour) with the … skills necessary to protect their IT systems and information assets'[2] and ensure that those target groups incorporate knowledge and skills into IT security action.

There is just too much information out there that is not tailored to the problem context of the user. Also, information on IT security and IT problems in general is often communicated in a way that requires more skills than everyday users possess.

---

[1] *Homepage of FISHA project, http://fisha-project.eu/*

[2] *See the EISAS Roadmap, https://www.enisa.europa.eu/act/cert/other-work/eisas_folder/eisas_roadmap*

In problematic IT security situations users often do not have the inclination, time, energy or cognitive resources to undertake a complete analysis of the situation. Where they are rushed, stressed, uncertain, indifferent, distracted or fatigued they tend to focus on less of the information available. When making decisions under these circumstances they often revert to simple heuristics taken from their experience in the analogue world or just do nothing.[3]

There is a long road to travel from knowledge to behaviour.[4]

- Firstly, it must be known that there are threats such as botnets out there in the first place.
- Secondly, one has to adopt the opinion that this is something that one should care about.
- Thirdly, one has to have the skills to actually do something to get rid of malware, such as botnet components on your equipment.
- If one then has the intention to actually invest time and energy in doing something then it is probably running the anti-virus software on the home PC (provided one does not have other more important duties to take care of in this available time slot).

[3] *Sternberg, Greg, 'The Psychology behind Security', ISSA Journal, April 2010; West, Ryan, 'The Psychology of Security. Why do good users make bad decisions?', Communications of the ACM, April 2008.*

[4] *See Ajzen, Icek; Fishbein, Martin, 'Understanding Attitudes and Predicting Social Behavior', Prentice Hall 1980, for an elaboration on the connection between attitudes and behaviour.*

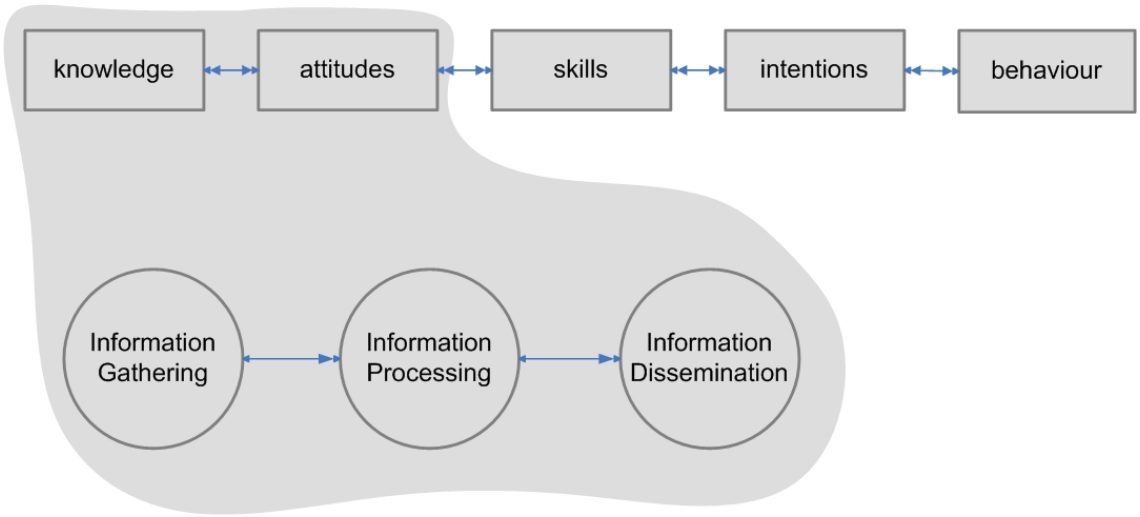


Figure 3 Information dissemination and IT security behaviour

There are awareness initiative websites addressing the home user. However, those initiatives compete with an abundance of information services to get the users' attention and are, additionally, difficult to evaluate in terms of effectiveness.

This illustrates that there is a real problem in reaching out with information on IT security to the home user and other entities without a professional IT department such as SMEs. Putting information on security websites is obviously not enough. The skill, intention and behaviour component of IT security behaviour at home is not covered.

The concept proposed here builds upon the recommendations of the ENISA Ad Hoc Working Group on Analysing Micro Enterprises' Needs and Expectations in the Area of Information Security (IS)[5], which point out that important steps are to create new user-friendly tools and tailor security and privacy initiatives in order for the target groups to be able to comply with them.

This study tests the presupposition that the easiest way to accomplish these aims is to take security information and alerts directly to the user's desktop instead of waiting until the user recognises that there is a problem and, in addition, has the motivation and opportunity to look for help.

[5] http://www.enisa.europa.eu/act/sr/reports/micro-enterprises

3 Goal of the study

The general goals of EISAS are to:

- **empower all EU citizens and SMEs** with the knowledge and skills necessary to protect their IT systems and information assets;
- **build on national capabilities** of EU Member States;
- **enhance cooperation** between national/governmental CERTs in the EU Member States.

The main objective of this feasibility study is to take the first step in the direction of the development and validation of a 'ready-to-use' information security awareness-raising concept ('EISAS Basic Toolset').

The EISAS Basic Toolset will be a methodology that facilitates outreach to the EISAS target groups with information about IT security in order to efficiently empower them with the necessary means and skills to protect their computers. The target groups are citizens (home users) to be reached via their employment in an enterprise.[6]

In addition, the EISAS Basic Toolset has the aim and should be a means of raising security awareness among home users, but implemented by targeting employees – *in their capacity as home users* – at their workplaces. This reflects the ever-increasing dissolution of the boundaries between work and private life, and also builds upon the fact that employees can be reached by motivating the employer to take an active role but home users cannot easily be reached directly. There is no reachability information on home users publicly available.

[6] *Regarding SMEs, among which the actual target group is the owner/managing director in that very capacity, it is recognised that this approach is not directly applicable. It is, however, with regards to employees of SMEs.*

4 Methodology

The study was planned and conducted as a feasibility study, as a proof of concept that an intervention such as the one described above would work.

The study was implemented using a 'pre-test –> EISAS intervention –> post-test' design.

The pre-test (an online questionnaire borrowing heavily from Eurostat Model Questionnaire on ICT usage in households and by individuals 2010) asked questions on IT usage, knowledge, attitudes, skills, intentions and behaviour regarding IT security at home.

The intervention consisted of a special website set up to inform respondents about botnets and 'how-to' information on getting the home PC clean. Also, a 112-Internet emergency button was presented that the respondents could optionally use to search the database for information and get in contact with support. After responding to the pre-test questionnaire, respondents were asked to go to the EISAS Toolset website, read the information, follow the instructions, and install the 112-Internet emergency button.[7]

For the post-test another online questionnaire was used, repeating some questions from the pre-test and also questions asking respondents to evaluate the EISAS Toolset information and the 112-Internet emergency button. The post-test was sent out to respondents of the pre-test.

This design shows the effect size of applying the EISAS Basic Toolset and will thus be a measure of impact (# of individuals taking desirable actions).

Pre-test, intervention and post-test were set up in German and Danish language versions. Undertaking the feasibility study in two Member States using two languages should show that the Basic Toolset would work on an EU-wide level.

In Germany participants were recruited among employees:

- of the two universities of Munich (Technical University Munich – TUM; University of Munich – LMU);
- from units of the public administration of the city of Munich;

[7] *See the section 'Overview of the information material provided' for a description of the contents of the website and the emergency button.*

- and persons connected to those institutions.

In Denmark participants were recruited among employees:

- of Alexandra Institute of the Aarhus University;
- of Danfoss, an international manufacturer of heating products.

Employees were invited by e-mail to take part in the study by a person known to and trusted by the respondents (CSO, head of department).

The pre-test was taken by 331 respondents; the post-test was taken by 108 respondents.[8]

[8] *For a more detailed description see section 6.2 Respondents*

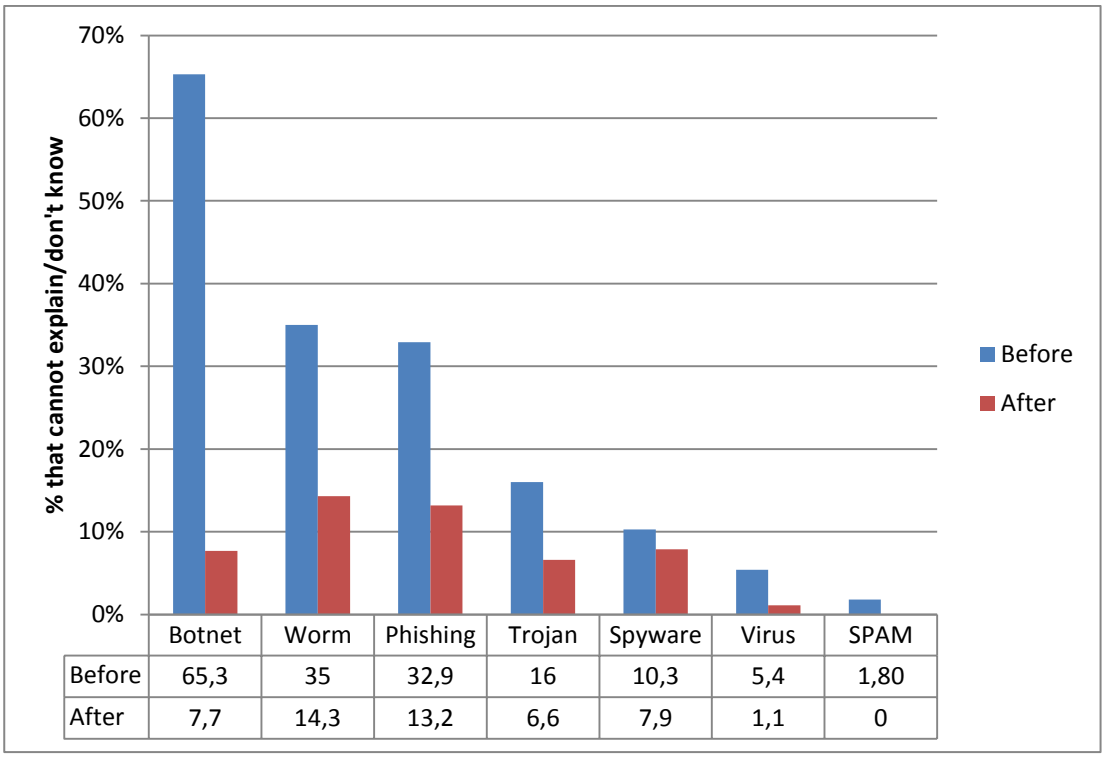
5 Results

5.1 Knowledge of IT security

The most impressive data, amongst the others, show that knowledge of what a botnet is proves to be dramatically absent even in this population of relatively well-educated citizens: 52.9% of the respondents stated that they do not know what a botnet is and 12.4% said that they cannot explain it to another person. This shows that there is a long way to go to make users aware of this threat.

But data also show a significant decrease of 'Do not know what it is' and 'Can't explain' responses after respondents digested the information presented by the EISAS Basic Toolset database. Only 5.5% of respondents claimed that they do not know what a botnet is and 2.2% said that they cannot explain what a botnet is to another person.

We see similar effects with the other terms. 'Don't know' and 'Can't explain' in the case of worms dropped from 35% to 14%, phishing from 33% to 13%, trojan from 16% to 6% and so on.



	Botnet	Worm	Phishing	Trojan	Spyware	Virus	SPAM
Before	65,3	35	32,9	16	10,3	5,4	1,80
After	7,7	14,3	13,2	6,6	7,9	1,1	0

Figure 4 Can you explain... to a friend or colleague?

The 'Introduction to Botnets' in the EISAS Toolset knowledge base worked remarkably well.

Why did the intervention work so well? Respondents liked the 'how-to' style of the presentation of the text and the security check that gave them the opportunity to actually check the security state of their PC at home.

As one respondent stated: 'It took me more than 15 minutes to fill out the questionnaire, 30 minutes at least, because I did not know some terms and what I have on my PC and had to think. But now I am much brighter than before.'

Another respondent wrote: 'The information contained in the toolset is worth much more than those 10 minutes you need to fill out the questionnaire. I downloaded and installed the firewall. The security check was positive all green then. May I forward the link to friends and colleagues? This is worth real money.'

Respondents learned and respondents acted.

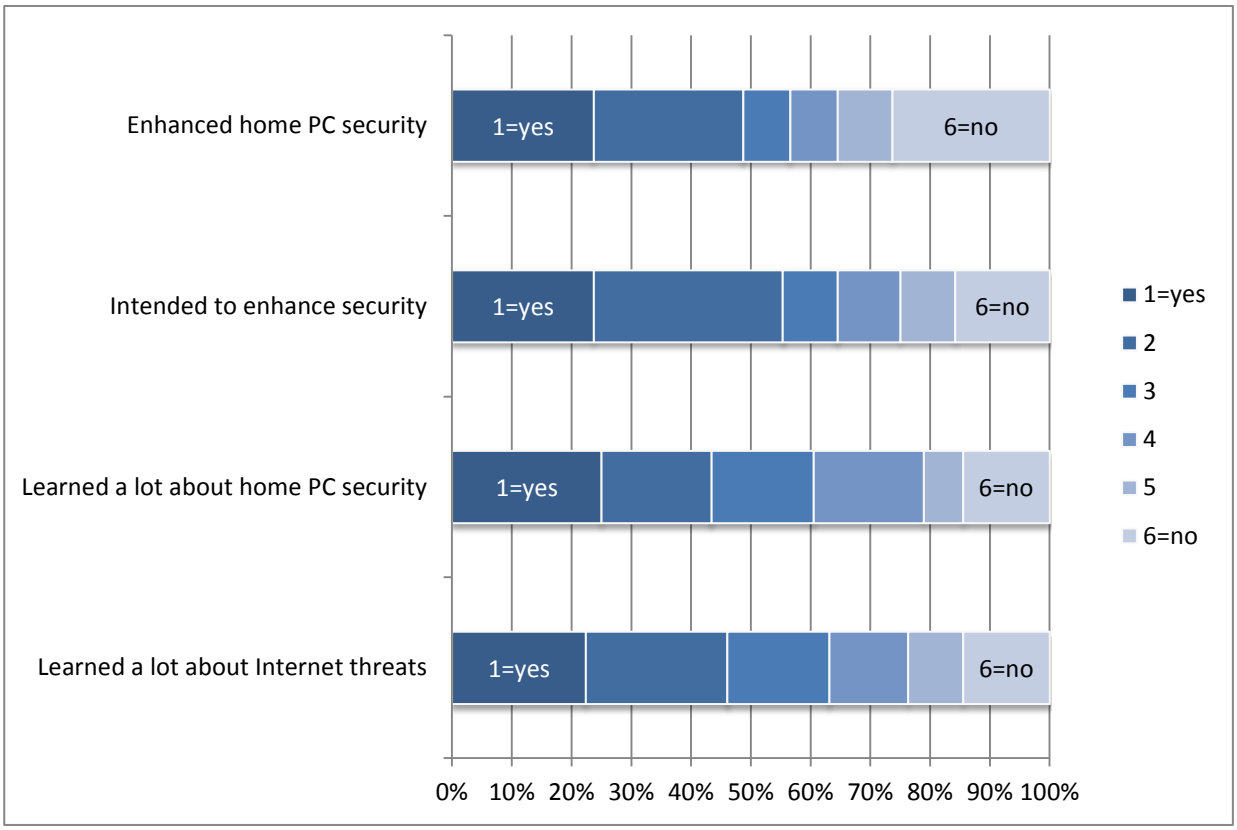


Figure 5 What effect did the 'Introduction to Botnets' have on you personally?

It can be seen that:

- 46% of respondents state they learned a lot about the threats of the Internet;
- 44% of respondents state they learned a lot about the security of their PC at home;
- 55% of respondents state that they intended to deal with the security of their PC at home;
- 49% of respondents state that they actually dealt with security and increased the security of their PC at home.

In other words, half of the respondents state that they cared about the security of their PC at home, actually increased the security and attributed this motivation and action to being exposed to the information and 'how-to' on the EISAS site.

As the content and wording of the Toolset introduction to botnets were directed at the less competent home user, we expected more effect on those low competence users than on users stating high competence with computers.

Figure 6 below shows the average rating of the items on a six-point scale running from '1=totally agree' to '6=do not agree at all'. Lower values signify that users agree with this item, higher values signify that users do not agree with this item.

Figure 6 thus shows that the Basic Toolset worked as expected. Users having a low level of competence with computers are showing much larger mean effects of the exposure to the toolset material. The largest effect can be seen with the item 'I intended to enhance the security of my private PC at home' as an effect of being exposed to the toolset material. This also holds for the item 'I enhanced the security of my private PC at home' as an effect of being exposed to the toolset material.

This is not only encouraging in putting further work into the EISAS Basic Toolset approach, but also shows that the attitude – intention – behaviour chain is working for IT security information. As far as we can tell from samples of some users who took part in the feasibility study, the behaviour change seems to be enduring. Users were impressed, changed their attitudes, changed their behaviour and are establishing the changed behaviour as a behavioural routine.

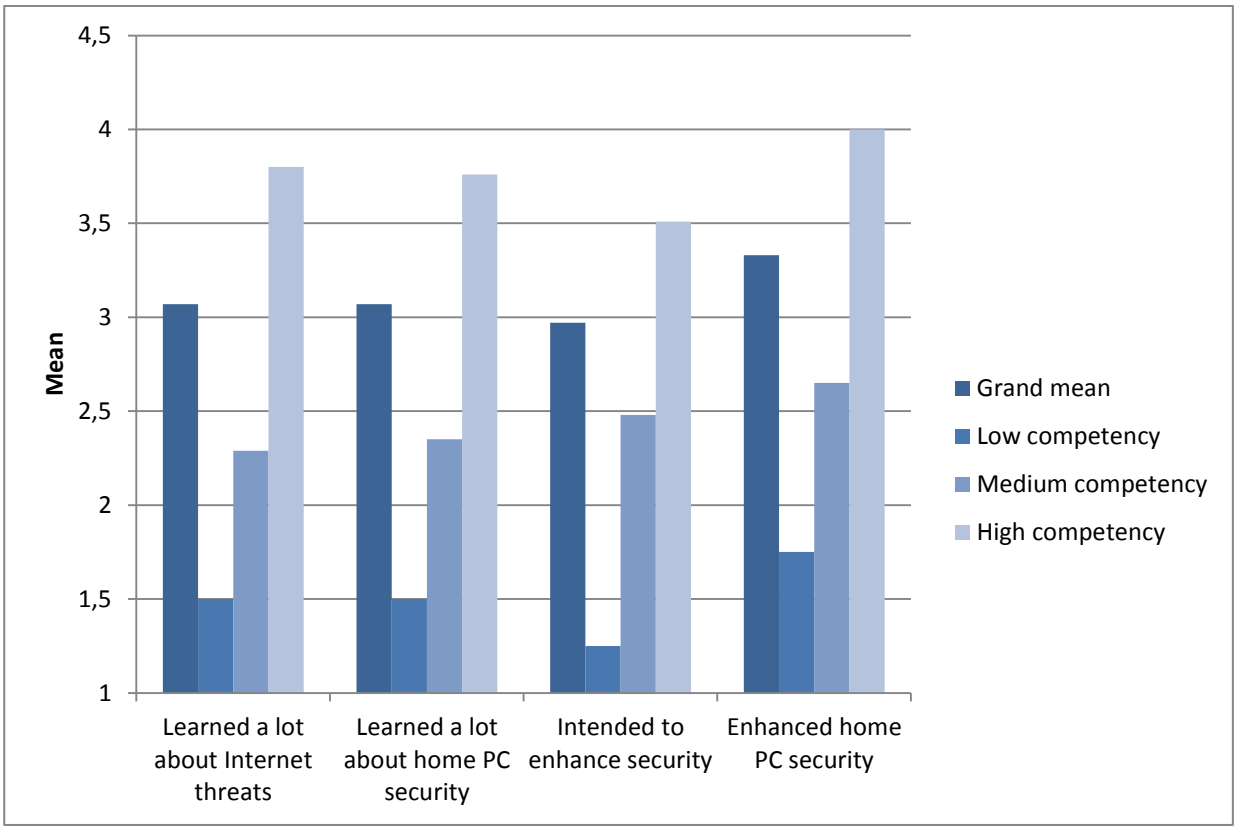


Figure 6 What effect did the 'Introduction to Botnets' have on you personally (mean values)

In general, respondents think they are reasonably well informed in the area of 'security in the internet' (see Figure 7). About 40% of the respondents state 'very good' or 'good' when asked how well informed they personally feel about 'security in the Internet'.

From the first to the second wave of the survey this figure goes up to about 70% feeling 'very good' or 'good' , the number of informed respondents grew by more than 30%. This shows that appropriate information such as in the EISAS Basic Toolset site does have an effect on the state of information of home users.

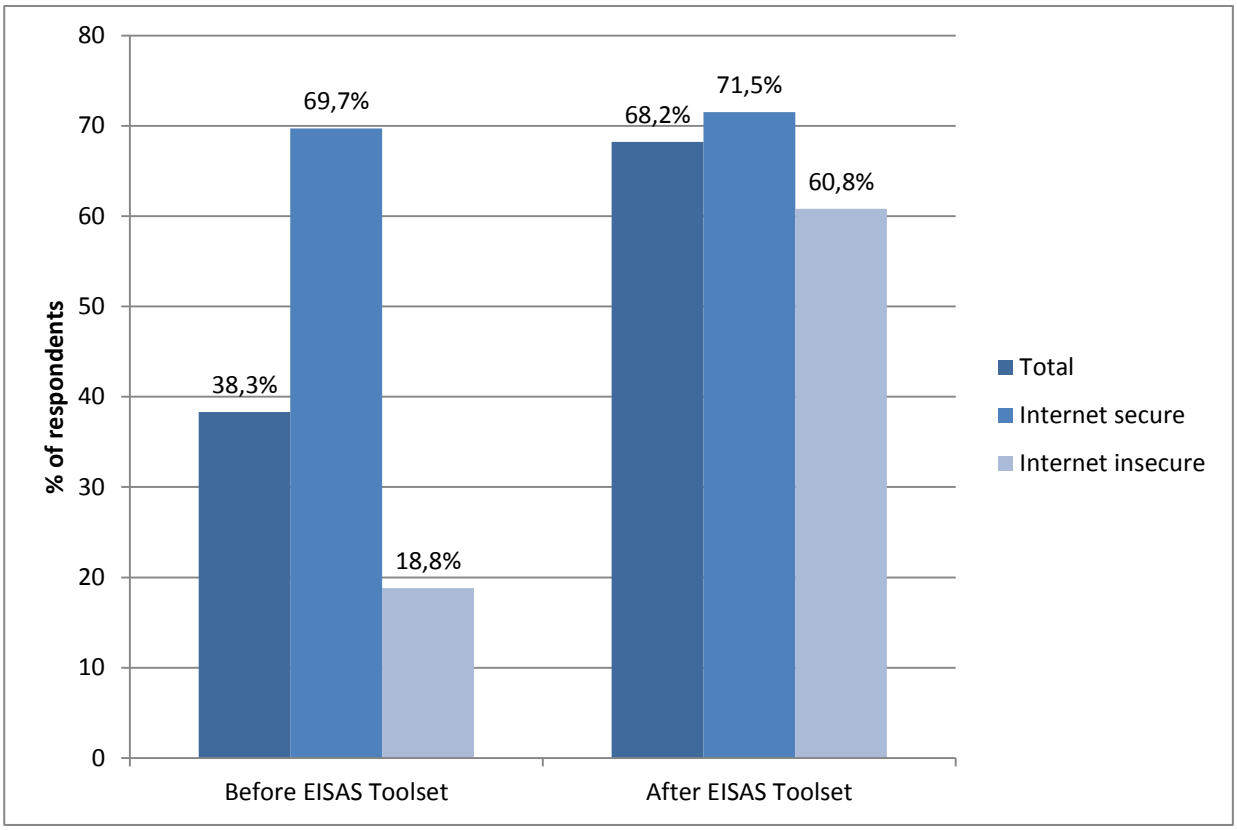


Figure 7 How well informed do you feel about security in the Internet?

Figure 7 also shows that those who think the Internet was a reasonably secure place feel better informed than those who feel the Internet was an insecure place. This probably reflects everyday reality: better knowledge leads to better mastery of the environment. Knowledge and perceived mastery are correlated.

It comes as no surprise that the effect on knowledge is larger with those who feel that the Internet is a less secure place. These respondents are simply more susceptible to messages that promise to change the feeling of insecurity. Even more interesting in Figure 7 is the fact that the information in the EISAS Basic Toolset not only changed the state of knowledge of those who feel that the Internet is an insecure place, but it also instilled knowledge in those who do not feel in too much danger from the Internet.

In light of the general goal of the EISAS Basic Toolset, this means that the awareness of home users can be changed to a large extent, *provided one can manage to get the attention and time of home users*. This may seem like a truism, but it shows that an awareness-raising activity extending the reach – the

right channel strategy, to adopt a term from marketing – is more important than accumulating information and hoping the users will find the right information at the right time.

Where do users head for information and solutions to security of computers and the Internet? Interestingly, Figure 8 shows that 'security sites on the web' are the most frequented sources of security information. Security sites on the web are sites such as BSI für Bürger[9] or Heise Online[10], but not security information of the producers of security products, which rank among the least preferred information sources on IT security.

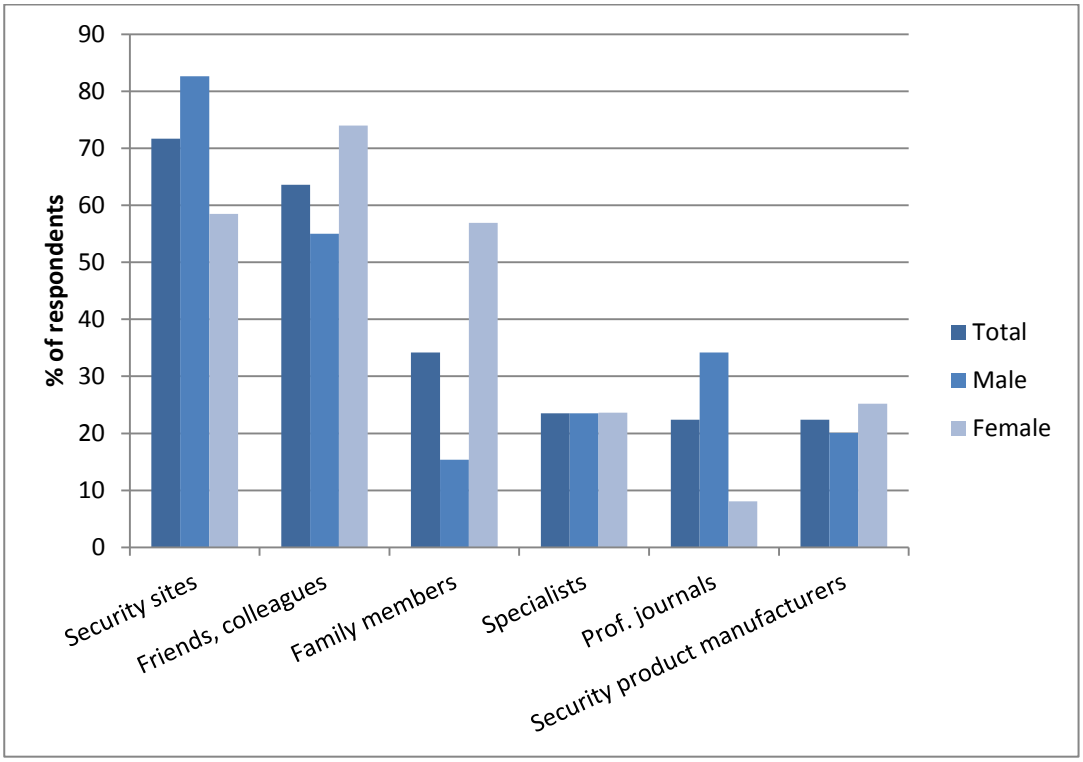


Figure 8 What sources do you use for information and solutions to problems of IT security?

[9] https://www.bsi-fuer-buerger.de/BSIFB/DE/Home/home_node.html

[10] http://www.heise.de/security/

Personal sources are very important to home users when it comes to information and support in the area of IT security and problems. Friends, colleagues, family members and specialists combined show that interpersonal sources are by far the largest and most important information source. This means that home users like information that has been filtered by some unbiased human intelligence.

Everyday information-seeking and problem-solving rely on a social network of persons who have more knowledge than the users themselves and are able to interpret the complex information out there in the context of the user's particular problem, knowledge and skills.[11]

Personal information, therefore, is easy information that poses little strain on the help-seeker. In fact, the problem will often be solved by the helping person. If an individual is in a position to use the help of a knowledgeable person, he/she will use it.

The combined importance of web and personal sources definitely shows what practitioners and governments have to do in the security education of home users: take information and personal support right to the desk of the user. The '112-Internet' browser plug-in, which was used as an experiment as part of the EISAS Basic Toolset piloting, does exactly this.[12]

5.1.1 Security information at the workplace

We had hoped that home users would bring home security information from the workplace, but this does not seem to be the case.

About 40% of respondents feel relatively confident ('1=fully agree' or '2') that IT security policies are known to all employees and 25% express severe doubts ('6=do not agree at all' or '5'). Equally, only 40% think that IT security policies are easily accessible. Thirty per cent of respondents agree when asked if the IT security policies included the home PC, but only 30% think that the policies are easily understood.

---

[11] *See Aspray, William, Haynes, Barbara M. (eds), 'Everyday information. The evolution of information seeking in America', MIT Press 2011.*

[12] *There are many other possibilities to get closer to the user at home and his/her needs, of course, and there are many surrounding conditions (legal, political, technical, ethical, security) that determine what would work. The crucial point, however, is that home users need a trusted source that can connect the problem at hand to their operational and task environment and offer help within the skillset and timing requirements of the user.*

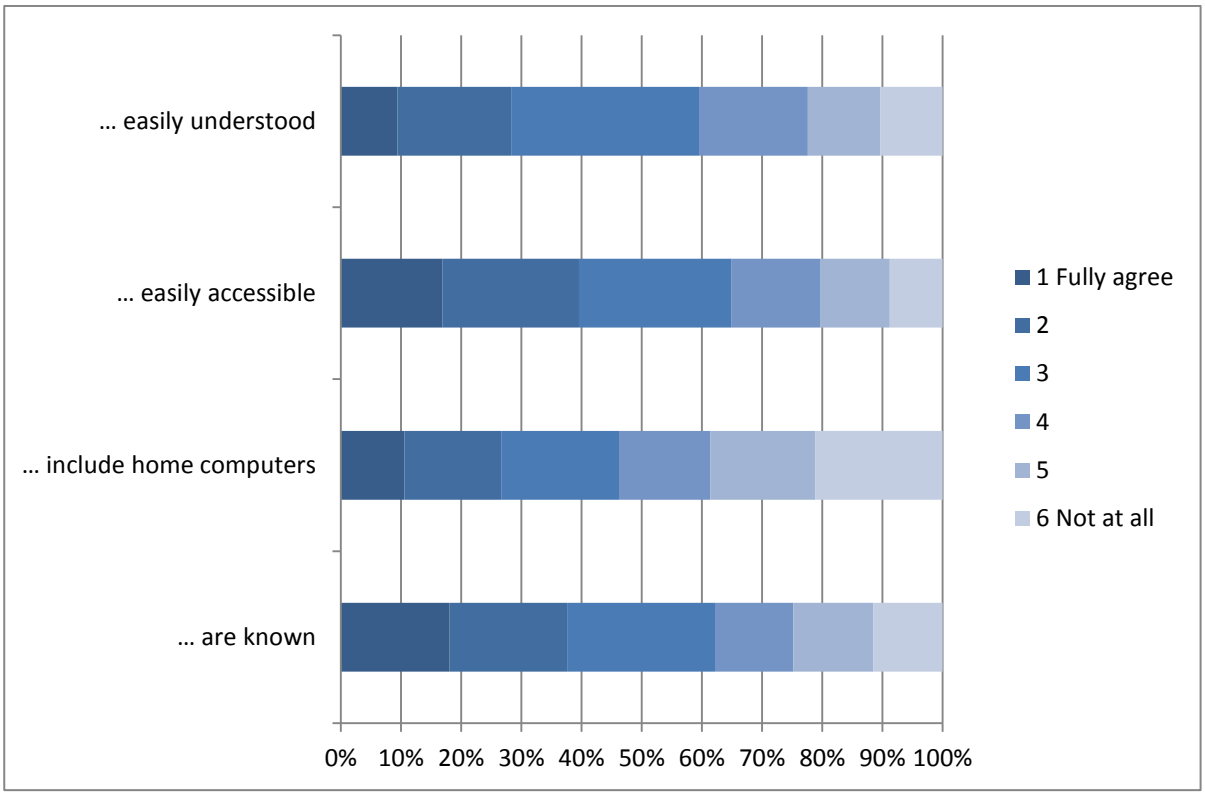


Figure 9 Security policies at the workplace are...

Users definitely think that the information security policies of their companies can be significantly improved. The evidence tends to suggest that company security policies are largely unknown and are not easily accessible. If an employee knows where to find them, they do not sufficiently include the security of home computers and if they do, the employee cannot understand what they are all about.

5.2 Attitudes towards Internet security and security experiences

Respondents were asked to state the biggest dangers of the Internet in their opinion and also how secure their PCs at home were against these dangers.

Figure 10 shows the arithmetic means of the responses to this question. The opinions of respondents were measured using a scale ranging from 1='not dangerous' to 6='very dangerous' and from 1='very secure' to 6='very insecure'. A high mean thus designates that the perceived danger of the Internet is high and – in the case of PC security – that the PC is perceived as insecure against this danger from the Internet.

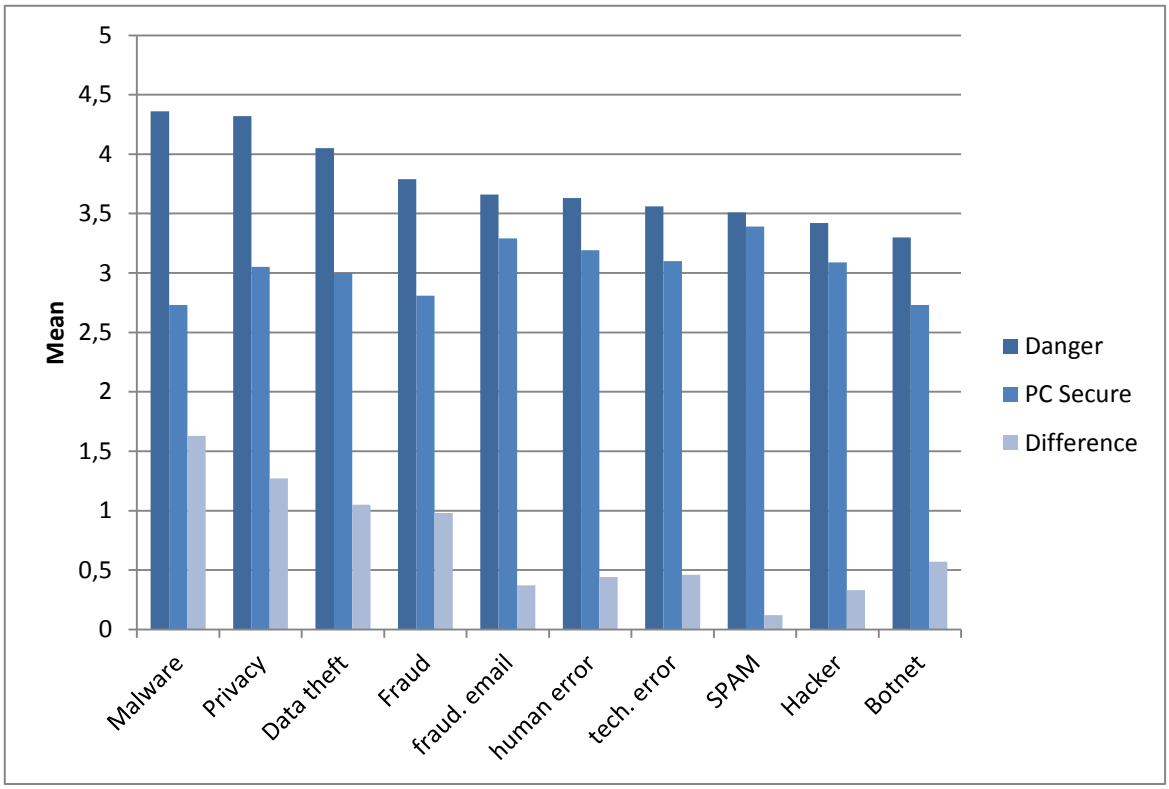


Figure 10 Biggest dangers of the Internet – how secure is your PC?

We see that respondents perceive malware (viruses, worms and so on), problems of privacy, data theft and fraud to be the biggest dangers of the Internet to the PCs at home.

At the same time they feel that their equipment at home is actually comparatively secure against those threats of the Internet. With malware, problems of privacy, data theft and fraud we find the greatest difference between perceived insecurity (danger) of the Internet and perceived insecurity of

the PCs at home. Malware, threats to privacy, fraud and data theft are perceived as the most dangerous threats, but respondents also think that they are secure in this respect.

The respondents feel insecure in the case of SPAM, fraudulent e-mail, human error, technical error and hackers.

Explanations of this outcome (the feeling of insecurity in those cases) can be found in the psychology of security, for example, neatly put together by Bruce Schneier.[13] The perception of risk is influenced by many factors such as innate tendencies, information on risks and actual experience with risks.

Figure 11 below shows the real world experience of respondents with regards to dangers with networked PCs. Respondents were asked whether they had had a problem with certain dangers and if they had actually experienced harm from those dangers within the last 12 months.

[13] http://www.schneier.com/essay-155.html, *'The psychology of security'.*

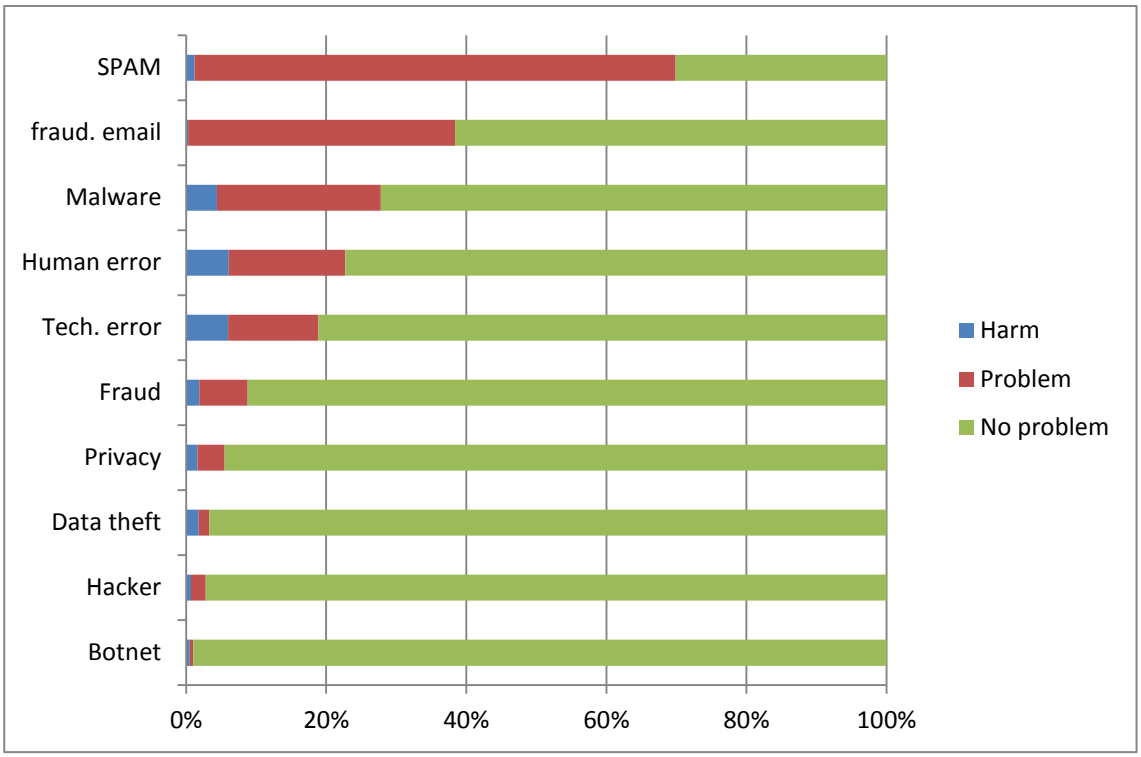


Figure 11 Did you have any of the following problems in the last 12 months?

SPAM really is a nuisance: 70% of the respondents say that they have had a problem with SPAM in the last 12 months and they feel that they cannot do very much about it. So this fact of the Internet has high salience (everyone gets SPAM): relatively low experience of harm done by SPAM and the experience that a user cannot do much about it. This leads to an intense feeling of the PCs at home being insecure against this threat.

Hackers are also seen as a risk one cannot immunise the home PC against. There is low real world experience with hacking, but users read a lot about this problem in the press. That is low salience, but high presence in the public discussion also leads to an intense feeling of the PCs at home being insecure against this threat.

It is interesting to see that human error, technical error and malware are seen as the threats doing most real harm to the PC at home. The difference in security perception is that people feel they are secured against malware (perhaps by installing an anti-virus package), whereas human and technical errors occur like bad weather (and one never carries warm clothing and an umbrella). So people feel insecure in respect to human and technical error, but not so much in the respect of malware.

Respondents do not report problems with botnets, they just feel insecure because of the coverage they may have seen somewhere or heard of botnets. It should be mentioned here that botnets were known to only 50% of the respondents in the first wave of the survey.

The information on dangers of the Internet presented in the Toolbox did have its effects on the perception and attitudes of the home users (see Figure 12 below). The mean fear of users regarding botnets rose by 0.85 scale points from the first to the second wave of the survey.

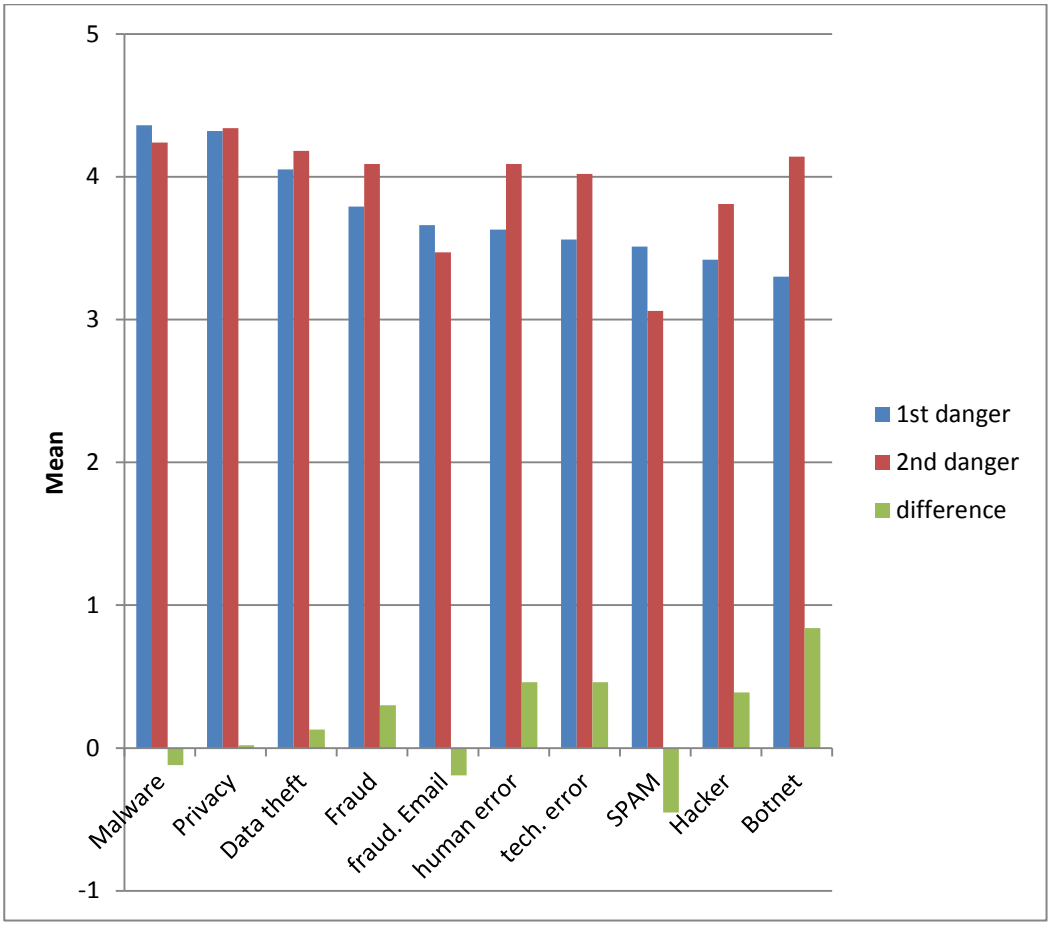


Figure 12 Change in **perceived dangers** of the Internet

Also, the fear of hackers – who are presented as the originators of botnets – grows significantly from the first wave to the second wave of the survey. In the same way, the fear of human and technical errors is greater in the second wave. The fear of SPAM is lower, probably because it is eclipsed by

other threats through technical or human error such as being seized by a botnet trojan or losing days' worth of work and data that cannot be recovered .

The information presented in the Toolbox did also have effects on users' perception of how secure their PC would be against the dangers mentioned (see Figure 13). In fact, after running through the Toolbox information on securing the home PC, users thought that their equipment is better armed against threats than before. There is one notable exception: users felt more insecure regarding botnets than before. Correlational analysis shows that less knowledge and less competence lead to a more intense feeling that the home PC could fall prey to a botnet or – perhaps – already has.

The explanation is that given the initial state of virtual ignorance regarding botnets, the information presented in the Toolbox shows users that botnets are a serious threat that needs to be addressed with proper security measures. This insight will last for a while and keep the botnet threat on home users' security radar for some time to come.

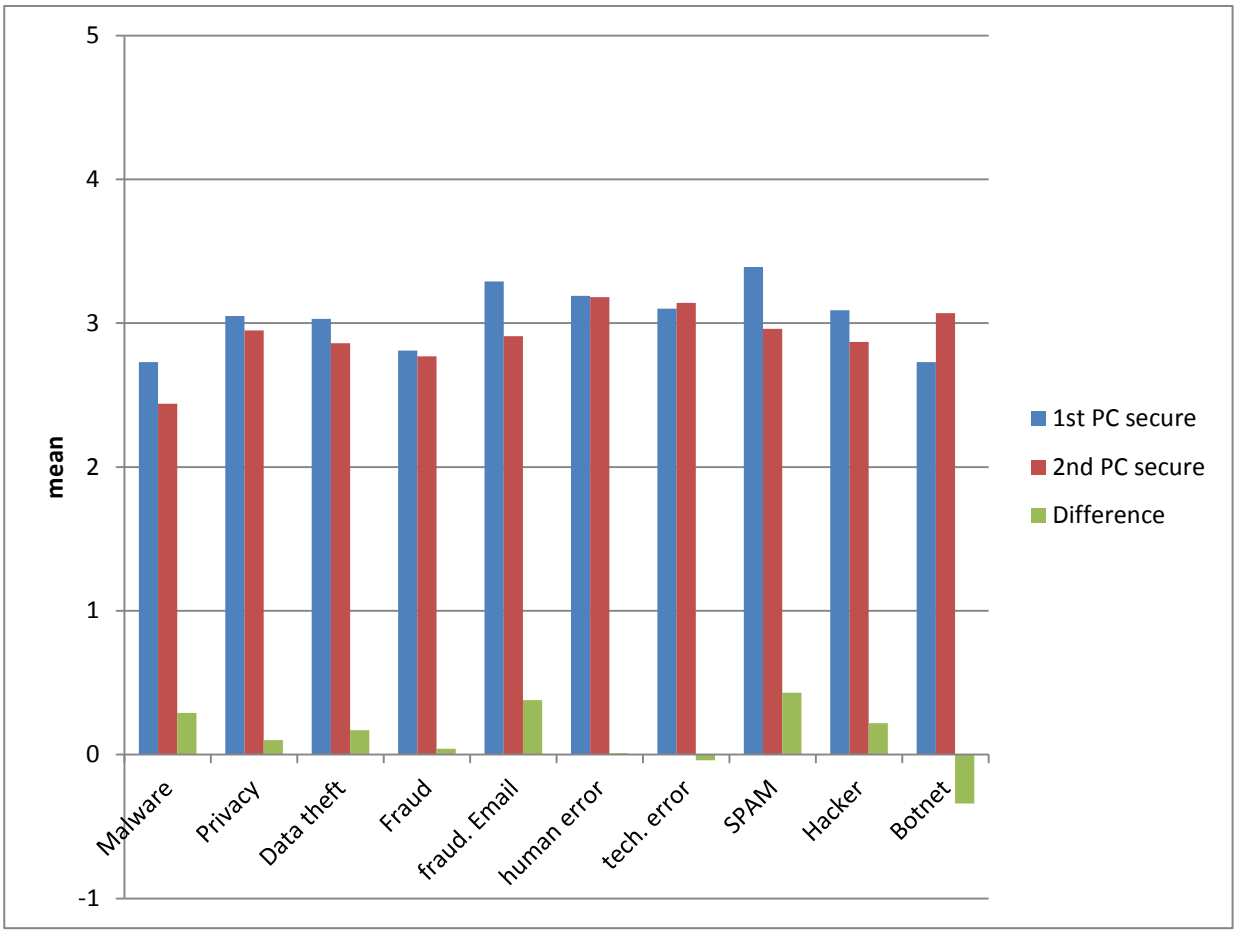


Figure 13 Change in **perceived security** of the home PC

What does this mean for the security education of home users?

It seems that the treatment of malware risks by home users has reached some sort of a stable state. People know that malware is there: 9 out of 10 have installed security software and what else can a home user do? It seems that here the security community has to come up with some new ideas if they want users to take more effective countermeasures against malware on their home PCs.

One inroad could be the botnet. The term is little known and if it is known, people think they should be concerned. This situation is a door-opener for doing something about security. The threat of botnets to society is primarily DDoS attacks targeting critical information services. If the large-scale DDoS attacks against society are equivalent to natural disasters in the world which people often learn about but seldom experience, then SPAM is the 'digital litter' all users unfortunately have to face every

day. Although 'digital litter' does not smell it is just like real litter; it is clearly visible to the user in the form of SPAM. The 'botnets-create-SPAM' relation, together with a sense of being indirectly personally responsible for the problem at large, may prove to be a way forward in convincing home users to better protect themselves.

5.2.1 Responsibility for security

Respondents were also asked who should care for the security of the Internet and should be held ultimately responsible. Respondents were asked to rank institutions, persons and bodies according to their responsibility. Figure 14 shows the percentage of respondents who ranked an institution, person or body with rank 1.

Respondents in this survey hold the home users, i.e. themselves, primarily responsible for the security of the Internet, closely followed by the Internet content providers. Producers of hardware and software are seen to rank 3 of those responsible for the Internet. Government and law enforcement definitely should not be involved, according to the opinion of these respondents.

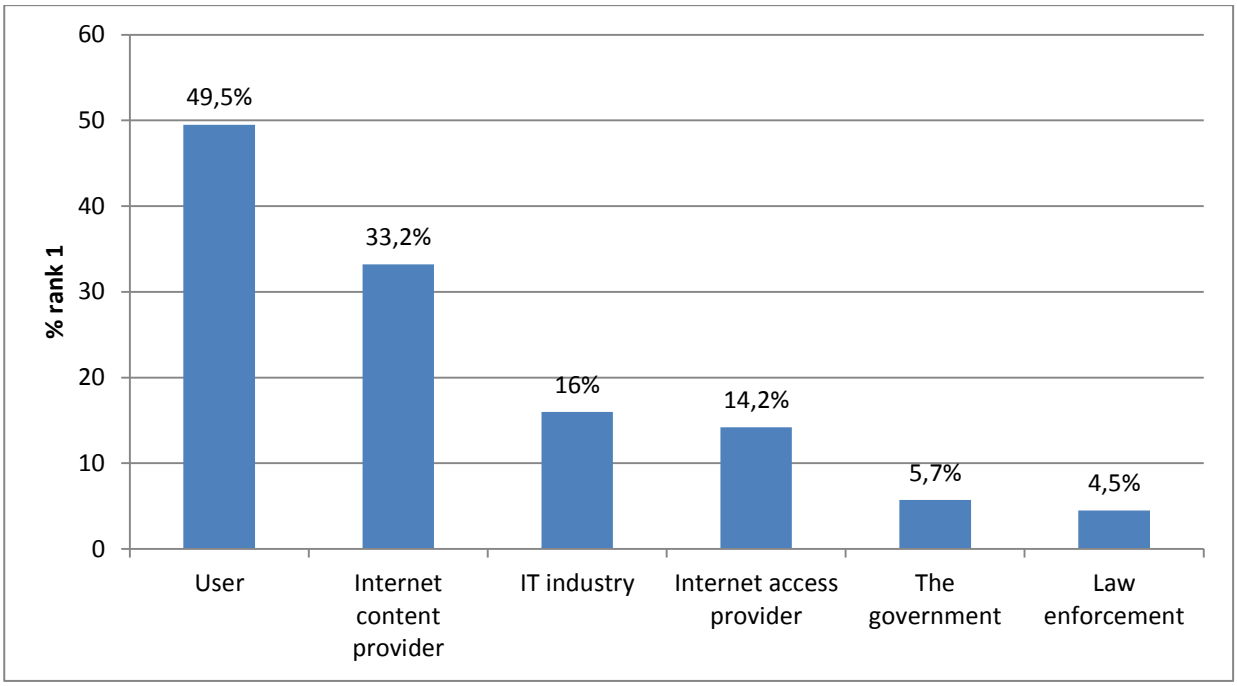


Figure 14 Who do you think should care for the security of the Internet?

The inclination of taking responsibility is underscored by the fact that 80% of the respondents agree with the statement 'it is in the social responsibility of the user to keep his PC clean'. This corresponds exactly with the ENISA report on botnets which recommends social countermeasures and states: 'From an ethical and social point of view, protecting a computer from malware is a civic duty.'[14]

Taken together this means that it is a good idea to take the users at home at their word and provide them with the information and tools necessary to put the intentions to be secure into practice. Users are definitely much more interested in being empowered to secure themselves than being secured from the Internet by police, government and Internet access providers.[15]

It is common knowledge among security professionals and the security community that the perceived time and effort necessary to secure home PCs is one reason why home users shy away from securing their networked IT equipment.

Four statements were suggested in order to surround this eluding topic of home user IT security:

1. Time and effort to secure my computer all-in-all is too high for me.
2. It is not important to know how security software works; just install it and you are done.
3. All-in-all the topic of IT security is too complicated for me.
4. There is definitely too much fuss around the topic of security in the Internet.

Respondents were asked to agree (1=totally agree) or not to agree (6=don't agree at all) to these statements.

---

[14] *ENISA, 'Botnets: Measurement, Detection, Disinfection and Defence', p. 130.*
https://www.enisa.europa.eu/act/res/botnets/botnets-measurement-detection-disinfection-and-defence

[15] *This outcome can be typical for German and Danish populations, of course. Whether home users in other Member States share this opinion is left to further inquiry.*

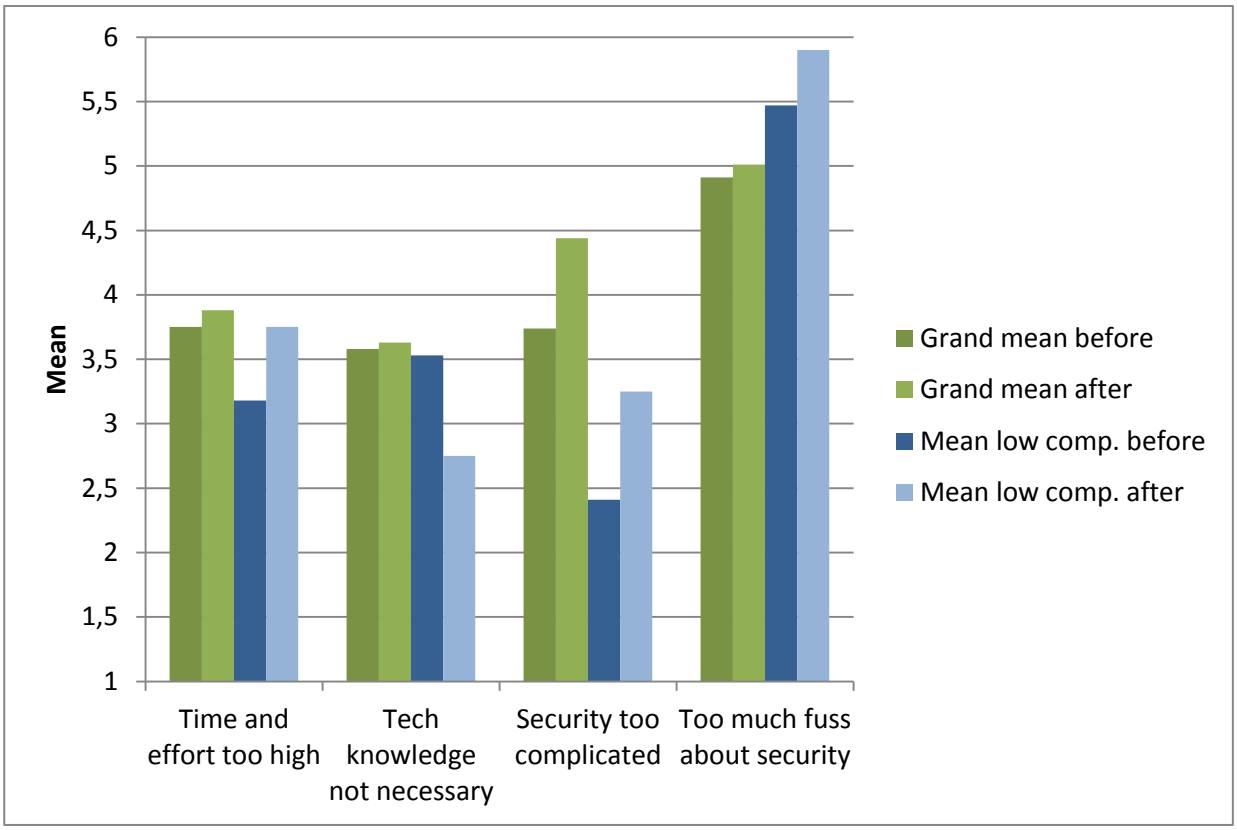


Figure 15 Attitudes regarding time and effort to secure the PC at home

The statement 'Time and effort to secure my computer all-in-all is too high for me' shows a grand mean of 3.58 on a six-point scale, suggesting that home users tend to invest more time and effort for securing the computer at home if they know what to do.

In this respect it is important that exposure to the Toolset is moving things in the right direction, most significantly for those respondents who attribute to themselves low competence with computers.

These respondents obviously learn that:

1. Time and effort to secure the PC at home is not too high.
2. Some knowledge of the workings of security software is necessary.
3. The topic of IT security is not so complicated after all.
4. The topic of Internet security is even more important than they thought before.

This shows that a lot can be done for the security of private computers in households if home users can be reached with the right information and the right tools. The EISAS Basic Toolset seems to be a step in the right direction.

5.3 Security behaviour at the home PC

Basically, respondents sport a security level known from Eurostat surveys, with 88.8% reporting that they have security software installed and 82% reporting that they keep the installed security software updated to the latest version and definition file.

Though security is on a high level already, Figure 16 below shows that it can be raised to even higher levels. Exposure to the EISAS Basic Toolset shows remarkable effects on the security behaviour of respondents.

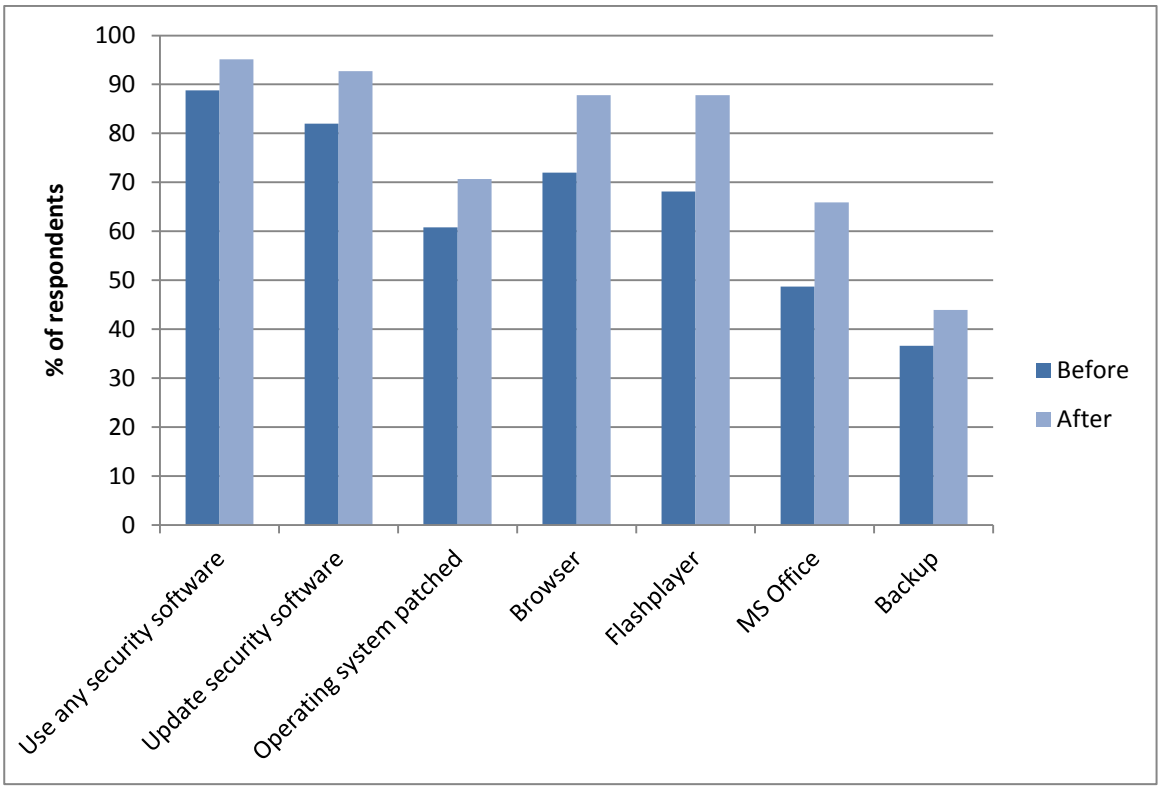


Figure 16 Security behaviour before and after intervention

Security software installed goes up from 88.8% to 95.1%, which is an increase of 6.3%. This is not too small an increase in itself, but taken into account that only 11.2% of respondents had the chance to change their behaviour, it means that 60% of respondents eligible changed their security behaviour.

Table 1 below shows the percentage of respondents having a certain security level before being exposed to EISAS Basic Toolset information and the percentage change to the better security level after they had worked through the Toolset information.

Action	% level before	% change after EISAS
Use any security software on my PC at home	88.8	6.3
Update my security software to the latest version and patch	82.0	10.7

Action	% level before	% change after EISAS
Operating system is on the latest patch level	60.8	9.9
Browser is on the latest patch level	72.0	15.8
Adobe Flash is on the latest patch level	68.1	19.7
MS Office is on the latest update	48.7	17.2
Backup always or often	36.6	7.3

Table 1 Change in security behaviour after being exposed to the EISAS Basic Toolset

For producers of security software it could be of interest that only one out of five respondents (16.9%) actually bought a security package; 10% installed a solution offered by the employer and 10% used a pre-installed package. All other respondents (more than 60%) state that they used some package available on the Internet free of charge.

5.4 Home and office

Many respondents work with office data at home. Two-thirds take home office data on portable storage or access office data using an online connection to the employer's network to work with. This is in line with the general observation that the borders between work and private life, between office and home are blurring.

One basic presupposition of the EISAS Basic Toolset is that there is a connection between employers and employees concerning the security of private computers at home and, in fact, this connection exists.

Of all employees, 89% consider it a good idea to have the employer provide information and tools for the security of private computers, smartphones, etc. at home.

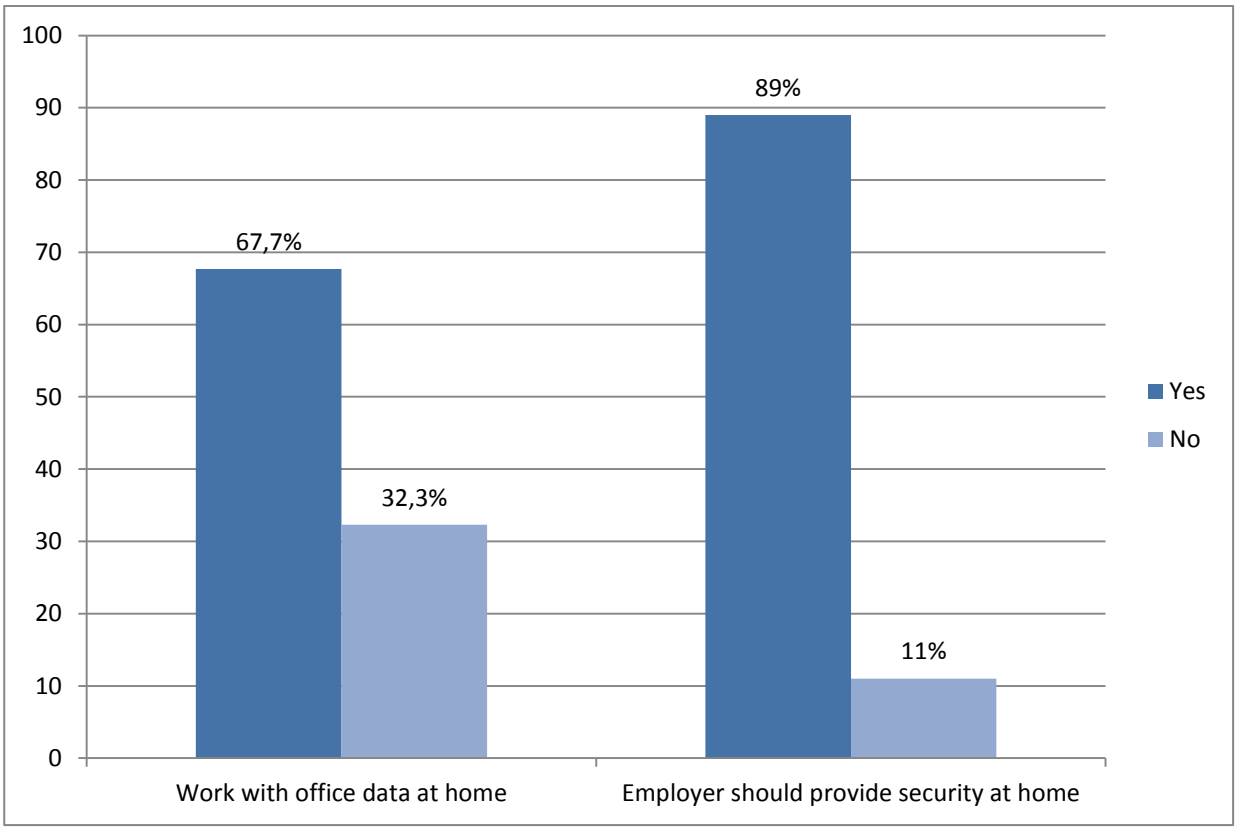


Figure 17 Office data on the home PC; should the employer provide information and tools for home PC security?

The reasons employees give for this opinion in an open text question are listed below.

- Since they work for the employer at home, it is a duty of the employer to care for the employees.
- It is in the interest of the employer to secure his/her information on home PCs.
- The employer is considered a trusted and knowledgeable source for information and tools.
- The employer could provide the right tools at lesser cost.

As one respondent put it:

'Though Internet security and IT security in general is ever present in the media most people act as if time and effort necessary were too high, updates would be annoying and security software just eating up PC resources. People who are not trained as IT specialists are unable to distinguish useful from

useless or even harmful information. On this background, it is a good idea to get the means for self-defence at home from an actor having a certain accepted authority (e.g. employer) who provides tools, background information and alerts if immediate action is required.'

Only a minority of respondents (11%) think that employers should keep their hands off the private home PC. Those users fear the employer could seize the home PC and do more harm than good to the employee at home.

The employees' requests and wishes regarding the security of their computers at home are currently not met at even the most basic level – the information security policies at the workplace (see Figure 18 below).

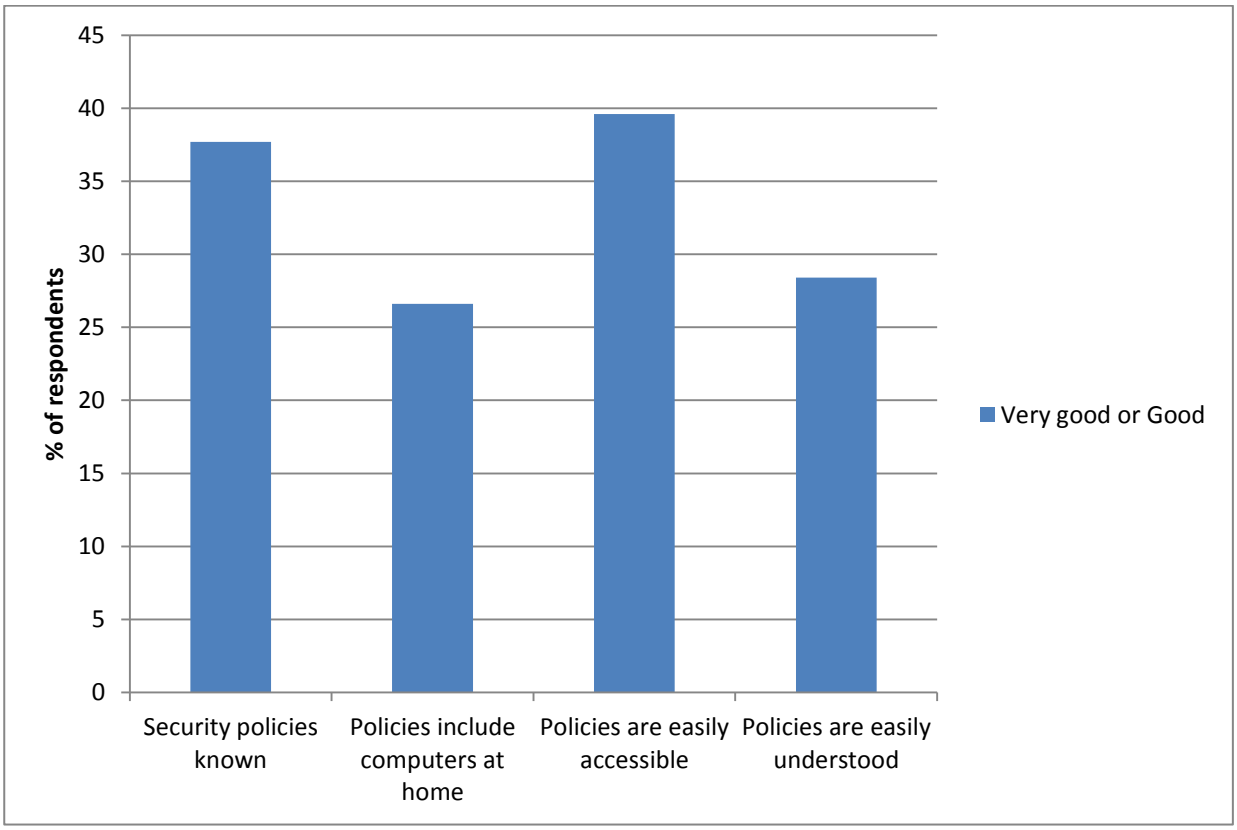


Figure 18 Security policies at the workplace and at home

- Only 37% of the employees think that the company security policies are known to all employees.

- Only 26% feel that the security policies of the company include the security of the computers at home.
- Only 39% of the employees rate the security information of the company as easily accessible.
- Only 28% judge the understanding of security information of their company as being very good or good.

On the whole this shows that there is much room for improvement in providing employees with security information they can act upon in their home environment.

Companies and organisations are trying to improve the situation. One participating organisation carried out experiments with a monthly consultation hour handling problems that employees have with their computers at home. Another implemented a series of lectures and presentations treating the problems of users at home.

Both approaches are considered successful in extending the reach of security information. However, on the downside, neither approach is considered suitable for large-scale implementation. Having a more personal face-to-face approach with security information and actually helping people in a 'home user helpdesk' is seen to be well beyond the resources available.

It seems that the EISAS Toolset has at least some properties of a mature solution in this regard:

- knowledge base with information tailored to the knowledge and needs of users (employees) at home;
- authoritative and trusted source of information and tools (employer);
- some method of providing personal or virtually personal contact to security specialists and tech-savvies;
- hints and alerts on what is important to reduce the complexity of dealing with IT security.

5.5 Attitudes towards the EISAS Basic Toolset

5.5.1 Introduction to botnets and securing the home PC

The 'Introduction to Botnets' site contained in the EISAS Toolset Knowledge Base was accessed over 1,500 times during the field phase of the survey. Since access to the site was anonymous there is no

information on who accessed the site and what information contained therein was accessed for how long. Whatever the users did, however, the introduction worked well, as was shown above.

Users also liked the introduction and its components. On a scale ranging from '1=very good' to '6=very bad', users on average rated content with 2=good, and its clarity even better with a mean rating of 1.8. What is even more important is that the lower the IT competence of the user, the more he/she liked the introduction to botnets. Since the text was tailored to the home user not having special training or experience in IT technology, the Toolset obviously worked in the intended direction.

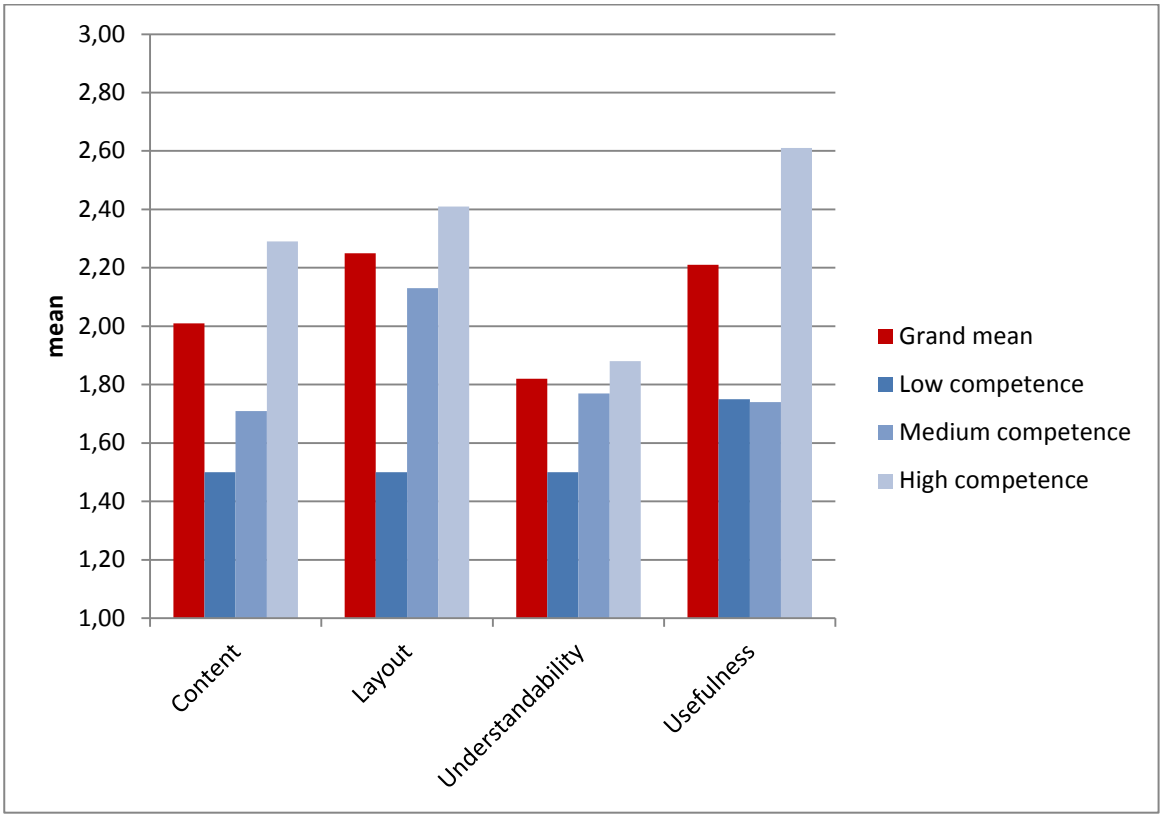


Figure 19 How do you like the 'Introduction to Botnets' in the Basic Toolset?

Users had many proposals for what content and problems could and should be included and handled in the Toolset database. The proposals covered issues such as:

- Is antivirus software really secure?

- What are the right steps if malware is detected?
- What threats exist against routers, smartphones, etc.?
- How can information be encrypted?
- How can a hacker be tracked down?
- How can I block and remove unwanted software?
- How can I filter content (children, advertising)?
- Secure online banking?
- What about the Mac?

It can be expected that the knowledge base would grow in many directions if home users were given the opportunity to question and discuss.

5.5.2 The 112-Internet emergency button

The experiment with an emergency button browser plugin (see Figure 20 below) was very well received by users (see Figure 21). On a scale ranging from '1=very good' to '6=very bad', users on average rated the basic idea of the emergency button with content with 1.2 and aspects such as layout, clarity, usefulness and usability with an average of about 2, which means 'good' on the scale of German school grades ranging from '1=very good' to '6=unsatisfactory'.

The questionnaire also asked the respondents about the perceived usefulness of various functions of the 112-Internet emergency button, which were also well received with average ratings ranging between 1.5 and 2.5 on a scale from '1=very useful' to '6=not useful at all'.

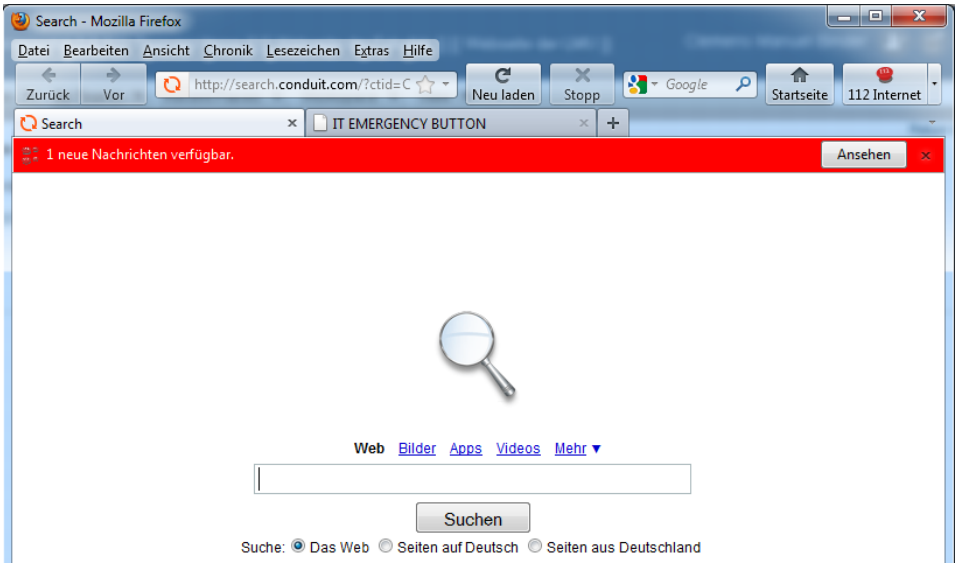


Figure 20 The 112-Internet emergency button with alert

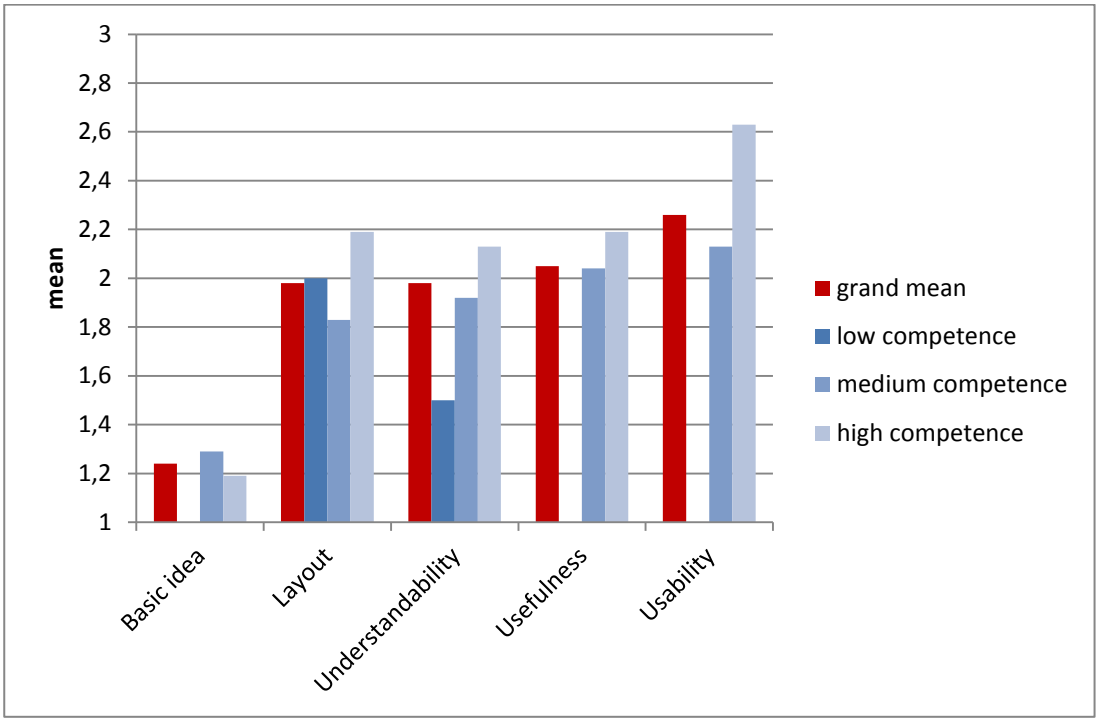


Figure 21 What do you think about the 112-Internet emergency button?

6 Participants

6.1 Companies

The study set out to reach a typical mix of companies and organisations. Among the companies accessed for participation were some large companies from the chemical industry, telecommunications and finance/insurance. In the public sector the study concentrated on the university and public administration sector.

All companies approached indicated serious interest in taking part in the study. Dealing with the IT security of employees at home is an issue. The timeframe of the study, however, was too narrow and in addition was located in the vacation time of Germany and Denmark. So participation was not feasible for most possible participants.

IT security is a high-ranking theme in all companies and organisations. Often it has to be routed through several boards such as staff council, human resources and IT, and it seems that in some cases the final decision would rest with top management. This process is laborious and time-consuming. In addition, the field phase of the study was scheduled for August/September. Summer is vacation time in Denmark and Germany so this severely derailed the smooth execution of the research programme. Eventually, the following institutions were able to participate in the study.

Initials	Name	Description
LRZ	Leibniz-Rechenzentrum	Large provider of network access and computing for academic institutions in the Munich area
TUM Inf	Technical University Munich	Technical University of Munich, Department of Informatics
LMU F11	LMU Munich	University of Munich, Department of Psychology and Educational Sciences
LHM	Landeshauptstadt München	Several units of the public administration of Munich
Other	'snowballing'	Employees of the above institutions gave the link to the survey to interested colleagues in the same and other institutions, friends and relatives
VKB	Versicherungskammer Bayern	Large insurance company

Table 2 EISAS Basic Toolset – Participating organisations and institutions in Germany

VKB was a special case. It was not able to finish the internal decision-making and preparation process within the timeframe allocated for the field phase of the study. Nevertheless, it decided to apply the EISAS Basic Toolset and since VKB decided to announce the project on the internal security website in the first instance, it was able to provide important information on the recruiting process and outreach of IT security information and tools.

Initials	Name	Description
AxD	Alexandra Institute	An institute under the Aarhus University focusing on IT and IT security, totalling 300 employees
DF	Danfoss	An international manufacturer of heating products in Denmark, totalling 6,500 employees

Table 3 EISAS Basic Toolset – Participating organisations and institutions in Denmark

Germany		Denmark	
Organisation	**# of Employees**	**Organisation**	**# of Employees**
LRZ	170	**DF**	6,500
TUM Inf	150	**AxD**	300
LMU F11	630		
LHM	370		
Other	900		
VKB	(6,500)		

Table 4 The number of employees in the participating organisations

6.2 Respondents

6.2.1 Demographics

The study was planned and conducted as a feasibility study, as a proof of concept that an intervention such as the one described above would work.

The table below shows some respondent characteristics used as independent variables in this report. The questions 'In your opinion: How secure is the Internet in general?' and 'How competent do you personally feel with handling computers?' were measured on a six-point scale and recoded to three categories for analysis (1,2 = green/high; 3,4 = yellow/medium; 5,6 = red/low).

Compared to the general populations of Germany and Denmark, demographic characteristics such as age and sex are skewed, reflecting the employee structure of the participating organisations (public sector, university, manufacturing and various other organisations whose employees were contacted by CSOs of the primary organisations participating in the study).

Compared to the general public, the participating respondents are, on average, younger, better educated and technically more proficient. Since the effects of the Basic Toolset are stronger with technically less proficient individuals, it is expected that extending the Basic Toolset to other organisations and other industrial sectors in a second, larger field experiment would produce average effect sizes of similar magnitude.

Demographic		Germany		Denmark	
		Count	*Column (%)*	*Count*	*Column (%)*
Age	≤20	14	6.0%	1	1.0%
	21 - 30	152	65.5%	10	10.1%
	31 - 40	27	11.6%	22	22.2%
	41 - 50	18	7.8%	34	34.3%
	51 - 60	13	5.6%	23	23.2%
	61 and older	8	3.4%	9	9.1%
Sex	Male	101	43.5%	83	83.8%
	Female	131	56.5%	16	16.2%

Demographic		Germany		Denmark	
		Count	*Column (%)*	*Count*	*Column (%)*
How secure is the Internet in general?	Green (secure)	10	4.3%	23	23.2%
	Yellow (moderately secure)	147	63.4%	66	66.7%
	Red (insecure)	75	32.3%	10	10.1%
Computer competency	High	111	47.8%	59	59.6%
	Medium	106	45.7%	38	38.4%
	Low	15	6.5%	2	2.0%

Table 5 Some demographics of the respondents of the study

6.3 Response rates: Survey 1

Survey 1 ran from 11.8.2011 through 30.8.2011.

Invitations to take part in the study were sent out by e-mail by a known and trusted person in the participating organisations (this was in the hands of the CSO). The invitees were encouraged to give the link to the survey to other people (colleagues, friends, relatives) who might be interested in taking part in the survey.

About 25% (N=729) of the individuals invited responded by accessing the online questionnaire. About 45% (N=331) of respondents completed the questionnaire. Of the N=391 respondents who did not complete the questionnaire, almost all (94%) quit with the first question asking for the respondent's e-mail address. Anecdotal reports show that some respondents just refuse to take part in a survey that is not strictly anonymous.

Revealing one's e-mail address definitely is a matter of trust. Respondents either put trust in the integrity of the institution doing the survey and the security of personal information in the hand of this institution or they do not.

If the response rate of 25% seems low, VKB gives a hint to the right perspective on response rates. VKB decided to invite employees via a link on the VKB security website. Here the response rate was just about 0.0006% (4 out of 6,500 employees). This is in line with one assumption of the EISAS study: it is just not much use putting a link to IT security information on a website.

It was not possible to test different incentives apart from e-mail invitation plus reminder by trusted persons in an organisation owing to the given restraints on time and budget for this study. But talking with the CSOs of the participating organisations and the evaluation of the toolset by respondents did reveal some possibilities (see *EISAS Basic Toolset*).

Survey 1	Germany	Denmark	Total	Completion	
				DE	DK
Invited	2,220	Unknown	N/A	N/A	N/A
Accessed questionnaire	524	205	729	23%	
Completed questionnaire	232	99	331	44%	48%

Table 6 Response report from Survey 1

6.4 Response rates: Survey 2

Survey 2 ran from 7.9.2011 till 19.9.2011.

Invitations to take part were sent out by e-mail to all who completed Survey 1. A reminder was sent out six days after the initial mailing. A total of N=108 respondents completed the second questionnaire.

Survey 2	Germany	Denmark	Total	Completion	
				DE	DK
Invited	232	99		N/A	N/A
Accessed questionnaire	95	36	131	41%	36%
Completed questionnaire	85	23	108	89%	64%

Table 7 Response report from Survey 2

7 Overview of the information material provided

7.1 Introduction to botnets and securing the home PC

Figure 22 shows a screenshot of the starting page of the Basic Toolset information on botnets and securing the home PC. The information presented is pulled out of a knowledge base, can be read onscreen or be printed out. There were seven paragraphs of information and a security check.[16]

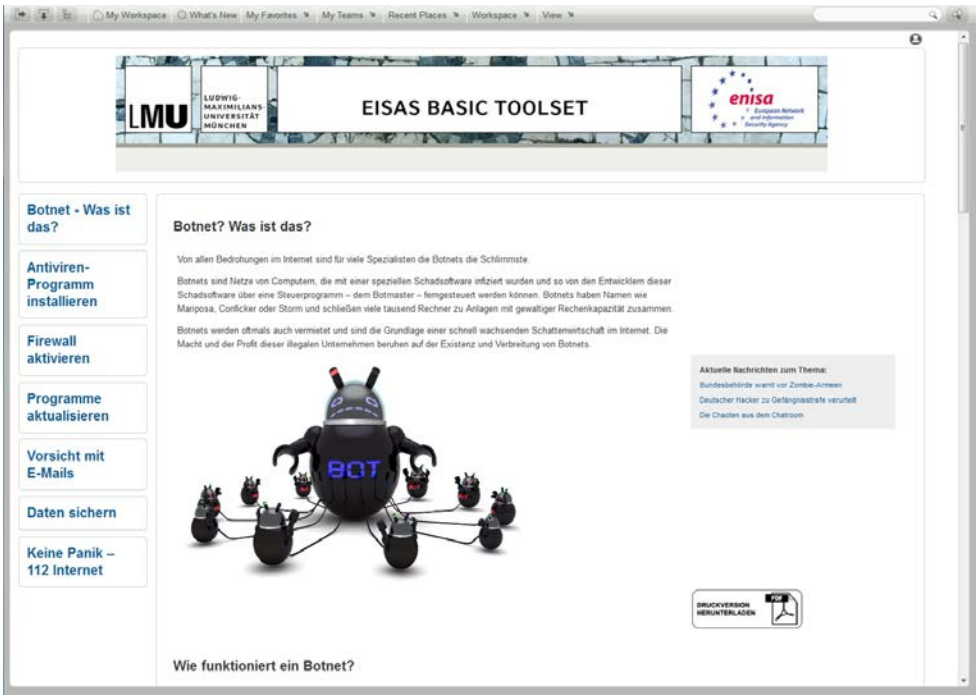


Figure 22 Start page of the Basic Toolset introduction to botnets and secure PCs

[16] See http://www2.computercheck24.com/visor_server/coronic2/de/audit-start.page

7.2 The 112-Internet IT emergency button

The 112-Internet IT emergency button was an experiment tested as part of the information material and is not an integral part of the EISAS Basic Toolkit 1.0. The experiment aimed to understand whether and how this approach would be received by the respondents. The component consists of:

- a browser plugin, communicating with the user;
- a dispatcher that stores and forwards user requests to a backend system;
- a Web 2.0 knowledge base that is configured as a background system, to a support ticket system, a chat server, whatever may have to be configured.

The browser plugin collects the requests of the user, transmits the requests to the dispatcher and transmits the help information from the dispatcher back to the user. If there are alerts being pushed from the backend system to a group of users or target machines via the dispatcher, the browser plugin informs the user like a traffic message channel and in this way works as an alert system.

The dispatcher works as a control centre that qualifies user requests and retrieves help from websites, databases, humans (experts, power users, IT buddies), whatever has been brought to the knowledge of the dispatcher.

The dispatcher component acknowledges the fact that there are many IT Sec information sharing and alerting systems out there and many ways information and alert dissemination can be implemented.

The dispatcher can collect information from various information, alert and help sources and transmits the search results to the browser plugin where they are shown on a results page. If the user clicks on a result he/she is connected directly to the information source. The dispatcher keeps track of what he/she delivered to what instance (browser, machine, user) of the plugin and asks the user (help-seeker) for feedback on the solutions and alerts received. In the simplest form, the feedback is a star rating; more elaborate forms can use a questionnaire.

In its current version the dispatcher connects to a Web 2.0 platform[17] as a knowledge base backend that contains information in various forms (FAQs, Wiki, documents, commented links, monitored

[17] *http://www.kablink.org/teaming was used for reasons of availability and convenience; every other Web 2.0 platform hosting a web-services interface would do as well. Teaming was chosen primarily because of its workflow capabilities which the project needed for tailoring and packaging IT help information.*

community forums, experts, power users etc.). For managing support requests it uses the OTRS[18] ticket system.

Other possible backend components already exist in the form of the many initiatives of CERTs, ENISA and other organisations. It can well be imagined that an 'Information Producer' in the FISHA model smoothly fits in here as the main information delivery backend.

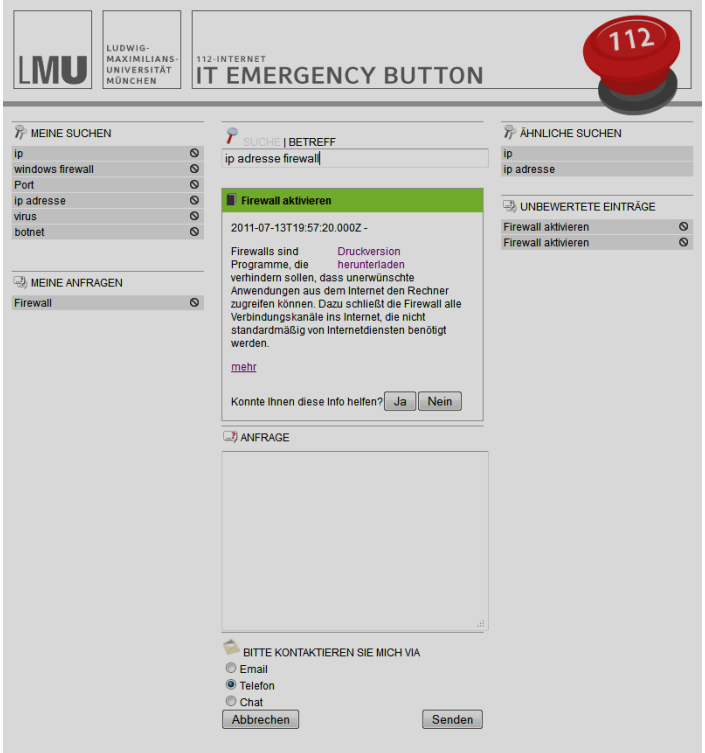


Figure 23 The 112-Internet IT emergency button user interface

[18] See http://otrs.org/

8 EISAS Basic Toolset User Manual

8.1 Overview

The EISAS Basic Toolset aims to bring IT security information out there to the end-user and his/her equipment at home.

Security information is collected and compiled by many organisations, whereby ENISA and the national CERTs have the obligation to compile and condense this information for national use. EISAS has the goal of finding ways of disseminating this information to the end-user at home and SMEs. The FISHA project can be seen as complementary to EISAS in the way that it shows ways to enhance the cooperation amongst the national information-providing bodies and organisations.

The EISAS Basic Toolset is set up to provide organisations and companies with recipes and support to enhance the outreach of awareness-raising initiatives to improve the security of their employees in their role of home users of private PCs and other networked equipment.

Ideally, the process consists of a security status check (comprising a questionnaire setting the stage), information, tools and other methods that help the home user to get along and a post-test that checks what was reached in the end.

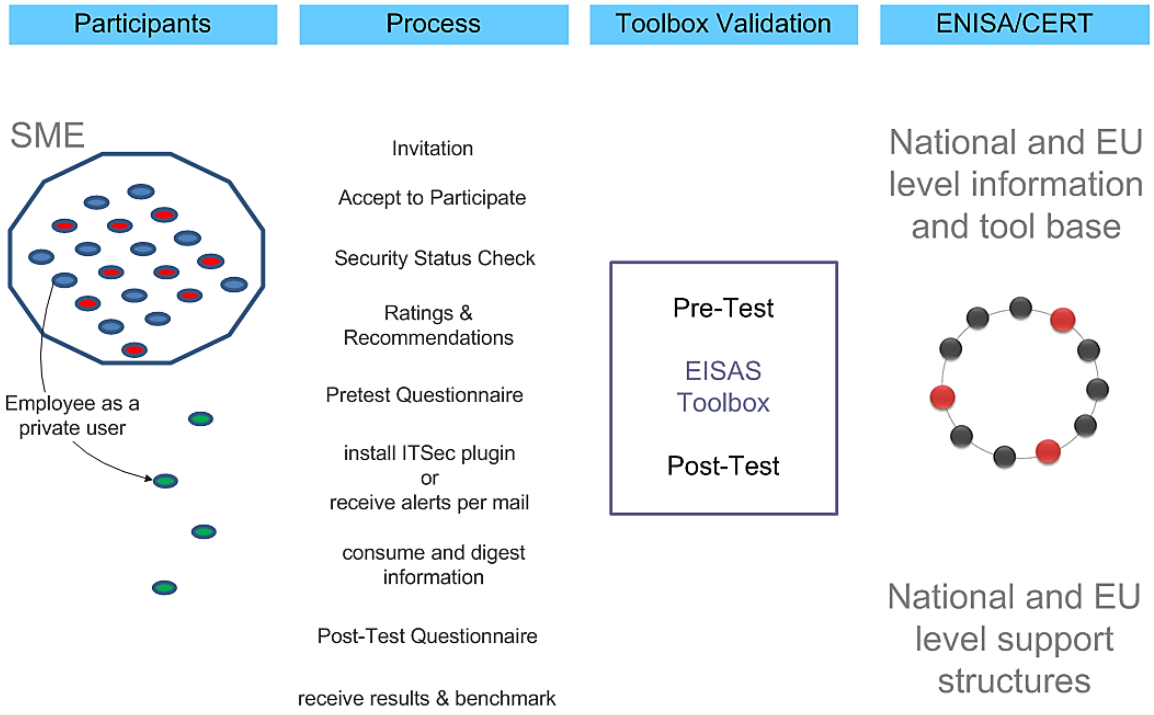


Figure 24 EISAS Basic Toolset blueprint

8.2 Recruiting participants

Recruiting participants is a two-step process. First, a company or an organisation has to be won for participation in the Basic Toolset program. Next the company has to motivate employees to participate and enhance the security of private IT equipment at home.

8.2.1 Organisations

Recruiting organisations and enterprises seems to be an easy, though time-consuming process.

Recruitment is easy if the organisation or enterprise has a security program in place. Running awareness-raising initiatives inevitably leads to the point where a lack of outreach and measured success is felt. All organisations and enterprises approached in the course of this feasibility study showed marked interest in new ways of reaching employees, refining and altering the channel strategy and measuring success. All organisations and enterprises were thinking of ways of enhancing the security practices of their employees in their role as home users.

Recruitment of organisations and enterprises can be time-consuming if the decision to take part in a programme such as this has to be taken to decision-making bodies and cannot be carried out by the

CSO under his own responsibility. If the EISAS Toolset is going to be part of the general IT security of the whole organisation or enterprise it probably has to be routed through several boards such as staff council, human resources and IT, and it seems that in some cases the decision finally would rest with the top management. This takes time. According to the experiences from this study the estimates run from three months to half a year for this laborious process.

Decision-making will be easier if the whole program can be carried out in-house. Taking parts of the program to cooperating organisations (LMU in this case) is a handicap owing to issues of data privacy protection and confidentiality.

8.2.2 Employees

Recruiting participants in the organisation or enterprise is a matter of finding ways to motivate employees to take part in this endeavour. The most important incentives seem to be:

- being personally addressed by a trusted sender;
- perceived usefulness of information and tools.

Putting a link to the Basic Toolset on a website does not produce any outreach. Luring employees to the Toolset via games or lotteries did not find much support when discussed with the participating CSOs, as they usually warn employees not to go to lottery sites or to take part in lotteries because of security reasons.

This feasibility study also shows that success in recruiting participants depends heavily on giving the respondents a feeling of being secure when taking part. Possible participants did not like to give away their e-mail address. Since measurability is a key component of the Toolset, it requires the inclusion of a 'before and after' assessment scheme. Therefore, additional incentives should definitely be considered to increase the motivation of employees to respond to both questionnaires.

8.3 Developing the questionnaire

The questionnaires used in this feasibility study had too many questions and took too long to get through for some respondents. Median completion time for the pre-test questionnaire was 15 minutes (meaning that 50% of the respondents took 15 minutes and less and 50% of the respondents took more than 15 minutes). Mean completion time was 25 minutes. The post-test questionnaire had a median completion time of 15 minutes and a mean completion time of 22 minutes. It seems to be a good idea to provide the participants with an EISAS model questionnaire from which the participants can take questions (following the example of Eurostat).

8.4 Knowledge base

In this feasibility study the EISAS Toolset stored the information presented in a professional knowledge base application. Though for simply presenting information this is a rather complex endeavour, it can be recommended. Built-in communication and feedback functions currently defining Web 2.0 seem to be the right way to foster communities of practice leading to empowerment and self-help for problems defined by home users themselves.

The experiment with the 112-Internet emergency button aimed to place a searchable information base (and in the future, possibly a network of tech-savvies) right in front of the users, always at their fingertips.

The information presented has to be tailored to the competencies and reading habits of the users. The Basic Toolset information on botnets can serve as an example. The amount of information, technical complexity and presentation style were well balanced to the needs of the respondents. Only time can tell what other populations and problem situations require.

As learned in the process of recruiting participating organisations, there is a wealth of knowledge on what works in a particular organisation (content, presentation of information, incentives, timeframes etc.) that should be collected, synchronised and put in the EISAS Toolset. Also, providing learning possibilities such as 'adventure-based learning'[19] for recurring security behaviour problems would be welcomed by enterprises striving to make their employees more secure at home.

A more streamlined communication between national CERTs and enterprises regarding advisories, alerts and early warnings would have favourable effects on building a knowledge base tailored to the needs and uses of end-users at home.

8.5 Results and benchmarks

The Basic Toolset assumes that measurement of success will be implemented on a regular basis. That means that there is an ever-increasing wealth of information on the security state of home users and their networked equipment at home. A benchmark showing the user where he/she stands in comparison to the average seems to be a good idea to express the importance of being secure to the home user and to further motivate him/her.

---

[19] *An example for solutions like this can be found at http://www.core-competence.com/en/*

9 Next steps

The feasibility study shows that the IT security of end-users and their IT equipment at home can be significantly improved using the EISAS Basic Toolset approach.

Citizens (home users) can be reached with information on IT security facts and procedures via their employment in an enterprise by motivating the employer to take an active role. The key factors for success are tailoring the IT security information to the needs and understanding of the end-users at home, and offering a support structure providing help at the time when help is needed. The EISAS Basic Toolset approach promises to be a way to efficiently empower end-users with the necessary means and skills to protect their computers and information assets.

To implement the EISAS Basic Toolset productively on a national and EU level according to the toolset blueprint in Figure 24, it has to be expanded and tested again.

The next steps ideally would comprise the following work packages:

- **Knowledge base:** The knowledge base has to be augmented to a state that qualifies as a home-user IT security portal. Important topics would be privacy and data protection, social engineering (fraud and phishing) and proper configuration of the various operating systems used on home computers. Also, the 'how-to' sections contained in the knowledge base have to be customised to the operating systems used on computers at home. There should be at least informal cooperation with the national CERTs to establish a stream of information, early warnings and alerts to the knowledge base.

- **User interface and functionality:** The user interface of the various components of the Basic Toolset should result in a seamless user experience. Here it is advisable to have a design guide comprising graphic assets and code snippets that can be reused in the various countries and enterprises. The functionality should comprise community-building features such as forums, blogs and similar features. Of course, quality insurance and the security of the Toolbox Platform itself would be an issue. In some cases, it may be a good idea to put the toolbox into the hands of a knowledgeable working group of the participating enterprise and consult on how to realise the EISAS Basic Toolbox in the enterprise without having to resort to networks and platforms outside the boundaries of the enterprise. Alerts and early warnings, though, could still be routed from the CERTs to the desktop of the employee as end-user at home following rules that can be defined between the participating organisation and national CERT.

- **Participants:** In the next iteration participating organisations should be selected according to the industrial sectors. The organisation should be visible and prominent to serve as a lighthouse project for other possible adopters in a particular industrial sector. It is advisable to have the EISAS

Basic Toolset working group build the next version of the toolset in tight cooperation with the lighthouse participant.

10 Acronyms

CERT	Computer Emergency Response Team
CII	Critical Information Infrastructure
CSO	Chief Security Officer
DDoS	Distributed Denial of Service
EISAS	European Information Sharing and Alert System
FISHA	Framework for Information Sharing and Alerting
IS	Information Security
NIS	Network & information Security
SME	Small and Medium Enterprise

P.O. Box 1309, 71001 Heraklion, Greece
www.enisa.europa.eu