Security and Privacy Awareness of Home PC Users in Norway

F.L. Andreassen and E. Snekkenes

Faculty of Computer Science and Media Technology, Gjøvik University College, Gjøvik, Norway
e-mail: einar.snekkenes@hig.no

Abstract

There is a growth in the use of consumer oriented internet based services such as internet banking. Some countries (e.g. Norway) have introduced citizen portals (e.g. MyPage – minside.no). These portals will give access to privacy sensitive data (e.g. health data). A recent survey of home pc security suggests that 90% of US home PCs are infected by some kind of malware. These infections are putting PC content at risk, may enable attackers to carry out internet banking fraud and may contribute to spam and botnet based attacks. Currently, most home PCs are shipped without active security features. This requires home pc users to enable, configure or install appropriate security measures themselves. User awareness of security issues is an important factor that can contribute towards better protection of home PCs. Indirectly, this can also reduce global and corporate security problems by making it more difficult to mount DDOS attacks and distribute SPAM. This paper reports on some of the results found in an investigation of home PC user security awareness. The results are obtained from a survey including 784 respondents in Norway. Our study suggests that there is a strong correlation between security awareness and the implementation of security measures.

Keywords

Privacy, security, awareness, survey, preventive technologies.

1. Introduction

Security of home PCs is of interest from several perspectives. Citizens want access to internet banking other financial services. This obviously requires security. However, there is a growing interest in delivering other personal services through citizen portals such as MyPage (minside.no). These portals may provide services such as access to social services, tax services, application for child day care and medical services (e.g. booking appointment, change doctor, access to medical records etc.). Again, the need for security may seem obvious. Taking a slightly different perspective, there are several hostile and undesirable activities where the home PC is contributing to bad behaviour (e.g. DDOS and distribution of SPAM). Consequently, from a global perspective, it is of significant importance to secure home PCs.

Unfortunately, securing home PCs is not trivial. One approach could be to require all PCs to be shipped with pop-up blockers, anti-virus, anti-spyware, firewalls installed and configured for optimum effectiveness. However, thus far, this option has not been chosen. This leaves it to the home PC user to decide what protective measures have to be taken and to implement these decisions. Some service providers (internet banks, ISP's) have started offering free security packages (anti-virus, anti-spyware and firewalls) to their customers. However, it is not clear if cost reduction of software will give the desired results.

Based on a survey of 784 respondents we have found a strong correlation between security awareness and the use of anti spy-ware, firewalls and pop-up blockers. This result suggests that one way of improving internet security would be to implement measures that increase the security awareness.

This paper is structured as follows: first we review related work on privacy and security awareness and the adoption of preventive technologies. In section 3 we present our survey and the questionnaire. The results of our analysis are presented in section 4. In section 5 we give some suggestions for further work. Section 6 concludes the paper.

2. Related work

In the context of citizen portals, we are concerned about both privacy and security. Our focus is on the relationship between privacy, security and the corresponding awareness. Below we give a brief survey of studies addressing privacy awareness, security awareness and the use of preventive technologies.

2.1. Privacy awareness

Privacy is not a new invention. The systematic discussion of privacy is said to be introduced in 1890, by Samuel Warren and Louis Brandeis in the article "The right to Privacy" in the Harvard Law Review (Warren and Brandeis, 1890). And later, in 1967 it was described by Alan F. Westin (Westin, 1967) to be the right to determine how information stored about us are spread.

The EU recognizes the importance of privacy (EU, 1995) (EU, 2002) and there have been several EU sponsored privacy related projects (PRIME, 2004) (FIDIS, 2004).

The abbreviations used in the following discussion and Table 1 represent the surveys from the Institute of Transport Economics citizens (ITE1 (Ravlum, 2005a), ITE2 (Ravlum, 2005b), Norwegian Board of Technology (NBT (Norwegian Board of Technology, 2004)), Norwegian Computing Center (NCC (Tjøstheim et al., 2001)), European Commission (EC1(European opinion research group EE/G, 2003), EC2 (EOS Gallup Europe, 2003)) , Software Innovation (SI (Griffin, 2005)) and the Urban Eye project (UE1 (Saetnan et al., 2004), UE2 (Helten and Fischer, 2004)). In (Andreassen, 2007) a more detailed discussion of the results from the surveys can be found.

Name	Type	Year	Location	Participants	Focus
ITE1	Citizen	2005	Norway	1000	Attitudes towards privacy
NBT	Citizen	2004	Norway	48	Electronic traces
NCC	Citizen	1999	Norway	11036	PII when E-shopping
EC1	Citizen	2003	EU	16124	Views on privacy
ITE2	Company	2005	Norway	424	Privacy vs. other interests
EC2	Company	2003	EU	3013	Privacy legislation
SI	Citizen	2005	Norway	509	User req. Mypage
UE1	Citizen	2004	Norway	218	CCTV
UE2	Citizen	2004	Germany	203	CCTV

Table 1: Reviewed security and privacy surveys (Andreassen, 2007).

According to the ITE1 and EC1 studies above, the Norwegian and Scandinavian citizens say that the general privacy issue is important to them and most are familiar with rights and duties stated by the legislation. But they do not have much knowledge of the relevant agencies and they trust most companies and organisations to comply with the legislation. The citizens trust the legislation to protect them and the Data Inspectorate to ensure compliance with legislation. We note that those who do NOT think legislation protects their personal data do not exercise their right to access to data about them any more than those who trust the legislation.

Similar findings are also reported by Aquisti and Grossklags (Aquisti and Grossklags, 2005), where people tended to overrate the immediate work or cost of protecting their privacy, for example by purchasing security software, in respect to the long-term privacy benefits. They were also inclined to choose short-term benefits in the form of discounts or special offers, in return for personal information that could damage their long-term privacy. At the same time, somewhat illogically, the respondents claimed to have high levels of concern for their privacy. This is also supported by the NCC survey.

We cannot avoid the discussion on how naive or uncaring the citizens are on the issue of privacy. In the ITE1 survey, 86% of Norwegians agree that only individuals with criminal intent have reason to dispute camera surveillance. This number is 67% from the UE1 survey and 70% in the UE2 survey. Also, in the surveys, statements like “but I do not write that sensitive e-mails” and “I do not have that kind of secrets [about the need for encrypting e-mails]”, suggest that people do not see the big picture of privacy. In addition, only 17% had ever heard of tools for limiting their tracks on-line and only 6% used them. This is also backed up by numbers from the EC1 survey, where only 12% of the sample use these tools. Common for users that do not use them, is perceived difficulty of installing and using such tools.

It seems then, that perhaps people have been affected by socially accepted attitudes towards privacy. That many say these things are important and that they say they know of legislation and their rights, but that the majority is not willing to do anything to actively protect themselves or be vigilant about their own privacy. This is reflected for instance by the small number of people that exercise their rights and the reasons they give for not doing so.

2.2. Security awareness and adoption of preventive technologies

Poston et al. (Poston et al. 2005) found that users are generally aware of spyware. But they are not motivated to take action or to pay for protection. Only 12% said they would subscribe to an anti-spyware service from AOL, should it be made available. Threat awareness figures in this study are; viruses (89%), spam (86%), spyware (75%), trojans (55%), worms (39%) and phishing (17%). Also, Schmidt and Arnett (Schmidt and Arnett 2005) found that 94% had known about the spyware threat for a year and 63% for more than 2 years. The surveys done by AOL/NCSA (AOL/NCSA, 2005) (AOL/NCSA, 2004), asked users about several of the terms used in this paper; the term spyware is very well known, as 91% in 2004 and 96% in 2005 had heard the term. But when the users where shown a list of what spyware were found on their computers, 90% did not know what the programs were and what they did. This is supported by Zhang (Zhang, 2005) who concluded that although most have many years of experience in using computers and the Internet, they know little about how to protect themselves from malicious software. "Most users know spyware is "out there", but are woefully lost when it comes to preventing it or removing it."

So it seems that the terms are becoming familiar, but users are still not very knowledgeable on the workings of spyware. But what will it take for people to act against spyware? To prevent spyware, people must understand how spyware operates and how they infect computers, and finally; they must be willing to make the effort of protecting themselves.

The surveys of Awad and Fitzgerald (Awad and Fitzgerald, 2005), and Freeman and Urbaczewski (Freeman and Urbaczewski, 2005) found which unwanted behaviours of spyware are most important to people; that spyware change settings on their computer, that it is drive-by downloading, that it is bundled with other software and that it is slowing down computer and causing crashes, but also that spyware threaten privacy and performance.

Hu and Dinev (Hu and Dinev, 2005) found the following as key to whether or not a user takes action against spyware; awareness of spyware, perceived usefulness of taking action, perceived controllability of the action, and perceived ease of taking action. Awareness of spyware is recognized as the most important factor, and was the only factor to directly influence the behavioural intention towards the adoption of preventive technologies. In another article, Dinev and Hu (Dinev and Hu, 2005) did further investigations into the importance of awareness in the environment of voluntary adoption of preventive technologies and awareness became the central determinant of user attitude and intention to act against spyware. Their findings indicate that awareness should be at the centre of information security policies and thus also in the work of getting the general public to fight the spyware problem.

2.3. Concluding remarks

Having surveyed works on privacy awareness, we found no authors reporting on any significant correlation between claimed privacy awareness and the use of anonymity tools. Dinev and Hart (Hu and Dinev, 2005) (Dinev and Hu, 2005) report that security awareness influences the adoption of preventive technologies.

3. The survey and questionnaire

For data collection we used a web survey. This was chosen due to its low cost and simplicity of distribution and transfer to a database. We judged the disadvantages of this approach (e.g. the risk of a biased sample) as small.

Recruitment was carried out as follows: We sent out emails to all Norwegian municipalities, including instructions and a link to a web page containing the questionnaire and more detailed instructions and information. In the e-mail, we requested the recipient to forward it to 10 employees in the municipality administration. The same e-mail was sent to the employees and students at GUC, and also friends, family, and partners in the PETweb (Norwegian Computing Center, 2007). project. The total population of recipients is estimated to about 7000 people.

The following groups were invited to participate (all above the age of 18 years): Civil servants working at Norwegian municipalities (452 * 10), Students and staff at Gjøvik University College (ca. 2000), Friends and family (ca. 500).

The survey consisted of 50 questions. Our questions can be grouped in the following categories; demography, security awareness, use of preventive technologies and questions about interest in security measures if these were made available from Mypage. The demography category included questions on gender, age, zip-code, education, employment situation, profession category, and experience with computers and internet usage. The security awareness category included questions on popup clicking, software installing, EULA reading, knowledge of threats, threat methods, security information from internet browsers, number of popups received per week, and automatic forwarding when surfing. The preventive technology category included questions on knowledge of preventive technologies, usage of preventive technologies, and updating software and OS. The final category, on interest in security measures from Mypage, included questions on educational material, information of threats, remote analysis and removal of malicious code from computer, and whether or not respondents would pay for these services.

The demographic questions were included for comparing the selection of respondents with the population of Norwegian internet users. The questions on surfing habits, knowledge of threats, threat methods, preventive technologies and updating/patching were intended to measure security awareness. Combining our security awareness measurements with our findings on the use of preventive technologies, we estimate their correlation.

Number of respondents	1086 people viewed the welcome page, 936 started answering questions and 784 completed their forms. This gives us a completion rate of 83.76% with 152 drop-outs. Average completion time was 9 minutes.
Gender distribution	47,8%(55%) men and 52,2%(45%) women.
Age distribution	Aged 18-24: 15.18%(25%), aged 25-34: 21.17%(22.5%), aged 35-44: 25.26%(23.13%), aged 45-54: 23.21%(19.38%) and aged 55-79: 15.18%(10%).
Education	Primary school: 2.17%(24.57%), secondary school: 20.92%(32.57%) and college/university: 76.91%(42.86%).
Computer experience	Under 2 years: 0.64%, 2-5 years: 4.21%, 6-10 years: 17.22%, 11-15 years: 33.55%, 16-20 years: 28.32% and over 20 years: 16.07%.
Internet experience	Under 2 years: 0.64%, 2-5 years: 16.45%, 6-10 years: 52.68% and over 10 years: 30.23%.

Table 2: Demographics on the survey participants

The demographics of our sample are given in Table 2. The numbers in parentheses represent the Norwegian Internet users, and were taken from an annual media use survey done by Statistics Norway (Statistics Norway, 2007). Unfortunately, comparable numbers for computer and Internet experience among Norwegian Internet users were not available.

The demographics presented in Table 2 show that the subjects in our sample are older and better educated than the average Norwegian Internet users.

4. Results

The questionnaire included 25 awareness related questions. After a reliability and validity analysis we decided to use only 9 of these. The other questions where not understood properly by the respondents and simply generated noise in the awareness score. See (Andreassen, 2007) for details.

We are focusing on the connections between the security awareness score and use of preventive technologies. One of the contributions of this paper is the establishment of a correlation between security awareness and actual use of preventive technologies.

4.1. Mean Awareness versus usage class

Each answer alternative on each awareness question in the questionnaire was given a value, e.g. 1 point for “I have never heard of this technology” and 4 points for “I can install, configure and use this technology”. We calculated the awareness score for

our respondents by adding the score on each of the nine questions selected by the validity and reliability analysis.

We found that age correlates negatively and education correlates positively with security awareness. See (Andreassen, 2007) for details.

We then grouped the respondents in 3 classes ("user", "non-user", "don't know") and compared the mean awareness score for each of these classes.

The analysis illustrated in Figure 1, shows significant differences between the three groups of respondents for all four preventive technologies. For anti spyware, firewall and pop-up blocker technologies, we found a linear significant increase from the "Don't know" group to the "No" group and from the "No" group to the "Yes" group. Antivirus, having an almost universal usage doesn't follow this pattern. Considering security awareness as a technology adoption motivator, the relationship between antivirus adoption and virus awareness would probably be less interesting as technology adoption here appears to be very high.

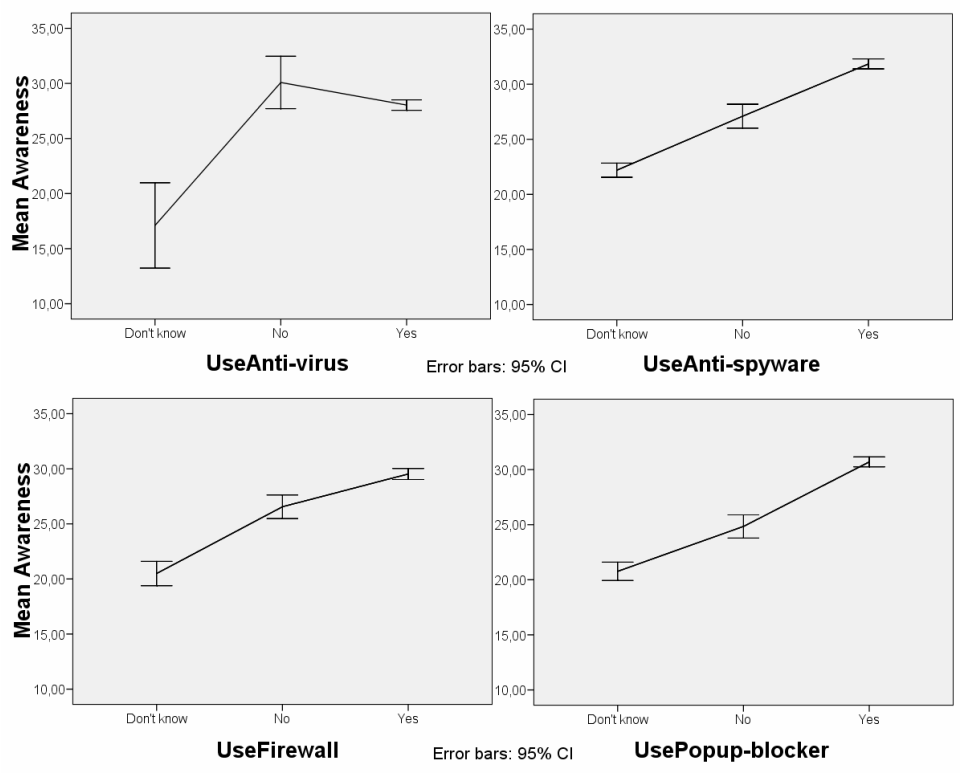

Figure 1: Awareness and use of preventive technologies

4.2. Connections between awareness and use of preventive technologies

We were interested in exploring the connections between security awareness and the use of preventive technologies. The values were 0.081 for anti-virus, 0.651 for anti-spyware, 0.599 for popup-blocker and 0.436 for firewall. All correlations were significant at the 1% level, except for anti-virus which was significant at the 5% level. Looking at the correlation between awareness and the four preventive technologies, we note low correlation on anti-virus and strong correlation between the other three.

We used linear and quadratic regression analysis to determine the effect awareness has on the use of preventive technologies, and found the quadratic equation performed better in our case. Our awareness score, using the quadratic equation, explains 3.2% of the variance in use of anti-virus, 42.5% of the variance in use of antispyware, 19.9% of the variance in use of a firewall, and 35.8% of the variance in use of a popup-blocker.

To confirm these theoretical connections between awareness and use of preventive technologies, we looked at the use of these technologies at different levels of awareness in our sample (Andreassen, 2007). We sorted the awareness scores from lowest to highest and looked at the use of the different technologies at these levels. The results are shown in Figures 2-6.

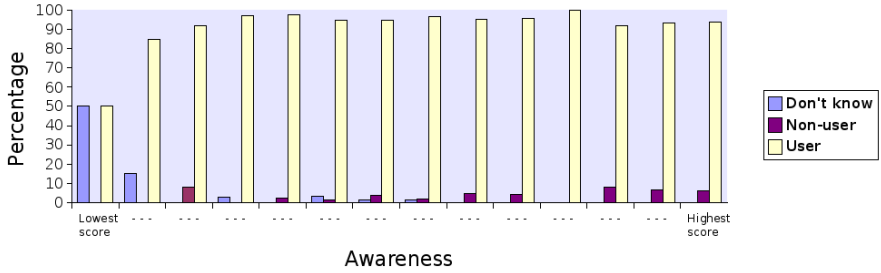

Figure 2: Awareness and use of anti-virus-tools.

Anti-virus is pretty much used by everyone (94.1%). And as we saw from the correlation and regression analyses, our measure of awareness does not explain the use of anti-virus-tools. We suggest this may be because the term "virus" is so well known by now, that "everyone" knows you need to use anti-virus. From the open question we learned that those who did not use anti-virus, justified their decision by claiming that their OS (Mac or Linux) have low vulnerability against viruses.

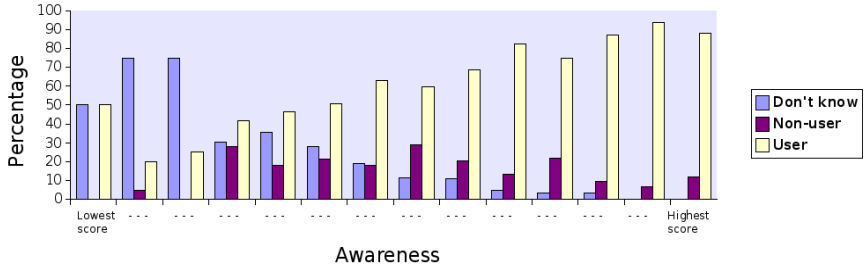

Figure 3: Awareness and use of firewall

Firewall is utilized by 72.3%. Here we see a steady increase in use as awareness increases. The high degree of penetration can possibly be explained by the fact that Windows has a built-in firewall, and also wireless routers and broadband routers often have a built-in firewall. From the open question we see that answers like "too little knowledge", "perceived difficulty of installing" or "too much hassle with access restrictions" are repeated for those who do not use a firewall.

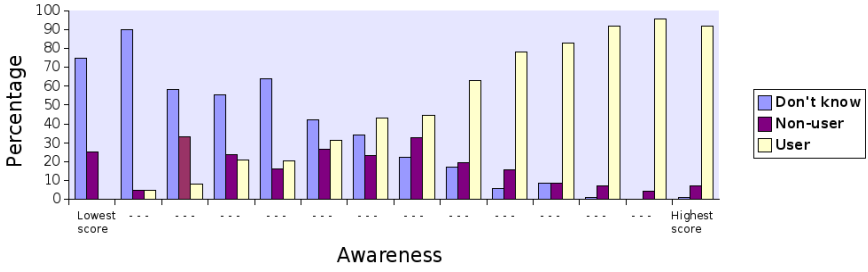

Figure 4: Awareness and use of popup-blockers

Popup-blocker is used by 66.5%. Also here we see a steady increase in use as awareness increases. One could perhaps expect that this number should be higher as major Internet browsers such as Internet Explorer, Firefox, Opera and Safari now have a built-in popup-blocker. From the open question it seems like lack of knowledge is the primary reason for why pop-up blockers are not used.

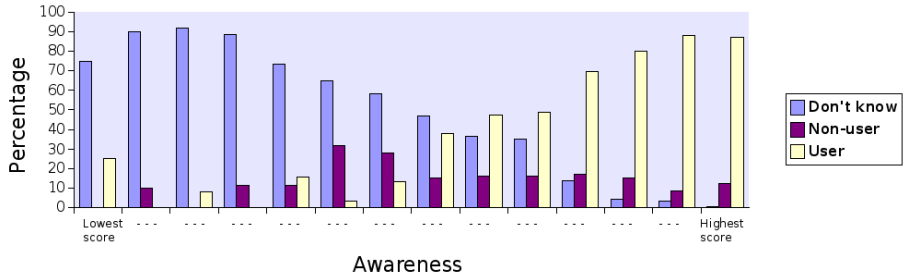

Figure 5: Awareness and usage of anti-spyware tools.

We see a steady increase in use as awareness increases. Use of anti-spyware is at 52.1%. The fact that only about half use anti-spyware is worrying. We quote (Thompson, 2005): "theft through spyware could be the most important and least understood espionage tactic today". From the open question we see that lack of knowledge on what it is, how to get and use such a tool is the main reason why people don't use anti-spyware. There is a large group of people not knowing whether or not they use anti-spyware (32%), so the actual usage might be somewhat higher e.g. because some are being unknowingly protected by built-in anti-spyware in other security products.

4.3. Trends in use at different levels of awareness

Figure 6 shows the result of computing the proportion of users of preventive technologies for each awareness level after smoothing. For most part of the curves (except anti-virus) we see a clear increasing trend in use as awareness increases.

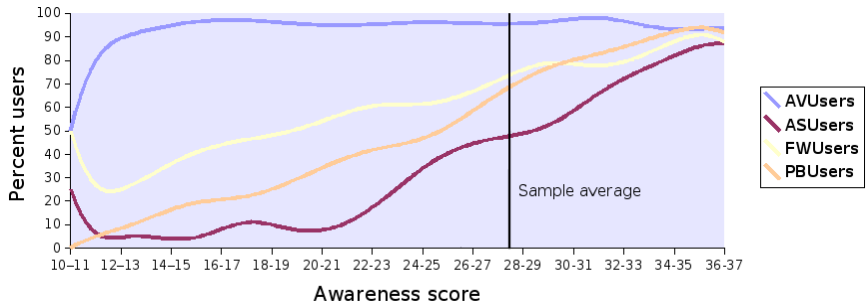

Figure 6: Preventive technology usage as a function of awareness

5. Future work

Our work should be extended and enhanced on issues relating to survey, sample and the associated analysis in the following areas:

- Improvement and expansion of the survey to gain more information about security and privacy awareness.
- Replacement of the self assessment of awareness by a more objective assessment.
- The use of scanning to determine if PCs are infected and/or have installed preventive technologies
- Improvement of the representativeness of respondents in the sample.
- More comprehensive factor analysis.
- Use of additional analysis techniques such as Structural equation modelling (SEM) techniques such as linear structural relation (LISREL) and partial least square(PLS).
- Investigation whether or not the use of preventive technology is self amplifying. i.e. are users of one protective technology more likely to adopt other preventive technologies?

When we asked about use of preventive technologies, we included an optional open question to why or why not the respondent used the different technologies. Only three respondents mentioned privacy as a reason for using preventive technologies. It seems that few associate the use of preventive technologies with privacy. Why is this?

We found a connection between security awareness and use of preventive technologies. But what is the nature of this connection? There were differences in the correlation and regression coefficients between awareness and the four technologies. Are there any underlying reasons for this, e.g. connection, such as technology sophistication, age, education? Further investigations into the possible underlying causes might lead to a better understanding of how the awareness affects the use of preventive technologies.

6. Conclusions

This paper has investigated the relationship between security awareness and the use of preventive technologies among home PC users in Norway. We have collected data using an internet based questionnaire. Our analysis shows that there is a clear relationship between awareness and the likelihood of using preventive technologies. Our results suggest that in order to reduce the number of infected computers and possible security incidents, at both individual, home, national, and global level, it will be beneficial to have a strong focus on security awareness.

Acknowledgements

The authors would like to thank the PETweb project partners, and in particular Lothar Fritsch, for giving valuable contributions. Simone Fischer-Huebner provided valuable comments on a very early version of the manuscript. Frode Volden provided help with the statistical analysis. This project has been sponsored by the Research Council of Norway under grant 180069/S10.

References

Andreassen, F.L. (2007), *Are the Norwegian Internet users ready for the new threats to their information?*, Master's thesis, Gjøvik University College, http://www.hig.no/content/download/9059/122138/version/1/file/Andreassen+-+Are+the+Norwegian+Internet+users+ready+for+the+new+threats+to+their+information.pdf, Last visited 28th May 2007.

AOL / National Cyber Security Alliance (2004), *Online safety study 2004*, http://www.staysafeonline.org/pdf/safety_study_v04.pdf, Last visited 28th May 2007.

AOL / National Cyber Security Alliance (2005), *Online safety study 2005*, http://www.staysafeonline.org/pdf/safety_study_2005.pdf, Last visited 28th May 2007.

Aquisti, A. and Grossklags, J. (2005), *Privacy and Rationality in Decision Making*, IEEE Security and Privacy, http://www.heinz.cmu.edu/~acquisti/papers/acquisti.pdf, Last visited 12th December 2007.

Awad, N.F. and Fitzgerald K. (2005), *The deceptive behaviors that offend us most about spyware*, Commun. ACM, 48(8):55–60.

Dinev, T. and Hu, Q. (2005), *The centrality of awareness in the formation of user behavioral intention toward preventive technologies in the context of voluntary use*, In The Fourth Annual Workshop on HCI Research in MIS, Internation Conference of Information Systems (ICIS), http://sigs.aisnet.org/SIGHCI/Research/ICIS2005/ SIGHCI_2005 _Proceedings_paper_5.pdf, Last visited 28th May 2007.

EOS Gallup Europe (2003), *Data protection in the EU*, http://ec.europa.eu/public_opinion/flash/fl147_data_protect.pdf, Last visited 28th May 2007.

EU (1995), *Directive 95/46/EC* of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

EU (2002), *Directive 2002/58/EC* of the European Parliament and of the council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications).

European opinion research group EE/G (2003), *Data protection*, http://ec.europa.eu/public_opinion/archives/ebs/ebs_196_en.pdf, Last visited 28th May 2007.

FIDIS (2004). *The Future of Identity in the Information Society (FIDIS)*, http://cordis.europa.eu/fetch?CALLER=PROJ_IST&ACTION=D&RCN=71399 accessed 12.12.2007.

Freeman, L.A. and Urbaczewski, A. (2005), *Why do people hate spyware?*, Commun. ACM, 48(8):50–53.

Griffin, E. (2005), *Minside behovsstudie / Mypage user requirements survey*, Vindfang AS.

Helten, F. and Fischer, B. (2004), *What do people think about cctv? Findings from a Berlin survey*, http://www.urbaneye.net/results/ue_wp13.pdf, Last visited 28th May 2007.

Hu, Q. and Dinev, T. (2005), *Is spyware an internet nuisance or public menace?* Commun. ACM, 48(8):61–66.

Norwegian Board of Technology (2004), *Holdninger til personvern / Attitudes towards privacy*, http://www.teknologiradet.no/Rapport_fokusgrupper_9-5lz.pdf.file, Last visited 28th May 2007.

Norwegian Computing Center (2007), *PETweb: Privacy Enhancing Technologies for web based services*, http://petweb.nr.no, Last visited 28th March 2008.

Poston, R., Stafford, T.F. and Hennington, A. (2005), *Spyware: a view from the (online) street*, Commun. ACM, 48(8):96–99.

PRIME (2004), *Privacy and Identity Management for Europe: The IST PRIME Project*, http://www.prime-project.eu, Last visited 28th March 2008.

Ravlum, I-A. (2005a), *Tøi-report 789/2005, Pinning our faith on big brother ... together with all the little brothers?* 2005. http://www.toi.no/getfile.php/ Publikasjoner/T789-2005.pdf, Last visited 28th May 2007.

Ravlum, I-A. (2005b), *Tøi-rapport 800/2005, processing of personal data in norwegian organisations*, http://www.toi.no/getfile.php/Publikasjoner/ T%D8I%20rapporter/2005/800-2005/T%D8I-rapport-800-2005.pdf, Last visited 28th May 2007.

Saetnan, A.R., Dahl, J.Y. and Lomell, H.M. (2004), *Views from under surveillance: Public opinion in a closely watched area in Oslo*, http://www.urbaneye.net/results/ue_wp12.pdf, Last visited 28th May 2007.

Schmidt, M.B. and Arnett, K.P. (2005), *Spyware: a little knowledge is a wonderful thing*, Commun. ACM, 48(8):67–70.

Statistics Norway (2007), *Norsk mediebarometer: Andel som bruker internett en gjennomsnittsdag, etter kjønn, alder og utdanning, i 2006*, http://www.ssb.no/emner/07/02/30/medie/sa86/internett.pdf, Last visited 25th May 2007.

Tjøstheim, I., Fuglerud, K.S., Boge, K., Arnesen, R.R. and Langaas, M. (2001), *Online-consumers and privacy*, http://www.nr.no/ingvar/Privacyreport979-2001.pdf, Last visited 28th May 2007.

Thompson, R. (2005), *Why spyware poses multiple threats to security*. Commun. ACM, 48(8):41–43.

Westin, A.F. (1967), *Privacy and freedom*, Atheneum, New York.

Warren, S. and Brandeis, L. (1890), *The right to privacy.*

Zhang, X. (2005), *What do consumers really know about spyware?* Commun. ACM,48(8):44–48.