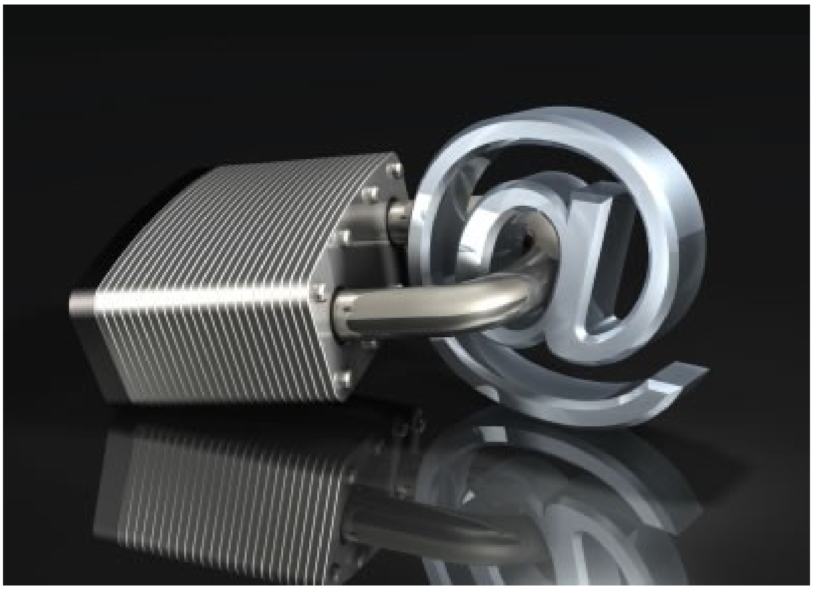
Safe Internet Use

How a Website Can Stimulate Internet Safety



Master Thesis

Philosophy of Science, Technology and Society
Science and Technology Studies

Author: Erik Baaij
First Supervisor: Dr. Ir. E.C.J. Van Oost
Second Supervisor: Prof. Dr. N.E.J. Oudshoorn

Date: 29-02-2012

Summary

The Internet is by now embedded in daily life. In our personal lives and in our society. It is an irreversible technology. But in it's relatively short existence it has created many issues concerning security and safety. These include issues towards personal information and it's theft and misuse thereof, and specific risks towards children like online bullying and grooming. To raise public awareness into safe Internet use, campaigns have emerged. However, research shows that the effects of these campaigns prove to be hard to realise.

Internet Safety is no longer established through technological fixes. It is partly, and mostly, achieved through safe Internet use on behalf of the user. In this thesis I analyse how a website can stimulate this behaviour from a Science & Technologies Studies point of view. The website www.veiliginternetten.nl from the Dutch government is used as case study and I hence ask the question how this website is designed and what effects it has on it's users. Veiliginternetten.nl was visited close to half a million times during the 2009-2010 campaign and is a website among many that are designed to increase Internet safety.

To analyse the website, I use a script analysis. This concept links the design and use of an artefact. It allows me to create a detailed look into the anticipated user, the design and actual use of the website. Using this semiotic approach I can analyse how the script from the website invites or inhibits certain behaviour towards their user.
For the empirical part of my research I used different type of sources. First, I held in-depth interviews with two core actors who were involved in the development and design of the website. Second, I analysed documents on the websites requirements that were produced in the course of its development, and documents that were used to anticipate the future user of the website. Third, I analysed the website veiliginternetten.nl itself. These three sources enabled me to analyse the script and to understand the social dynamics of the design process during which the envisioned users and the websites script were constructed.
Finally, I did a small qualitative empirical experiment on the real use of the website. I selected four envisioned users from the campaigns target group who had no prior experience with the veiliginternetten.nl website (however all had general Internet experience). These respondents were asked to visit veiliginternetten.nl and to acquaint themselves on Internet safety. The respondents were interviewed twice: once before their actual use and then a week later after their use of and experience with the website. This allowed me to learn about how the script of the website was read by real users.

My analysis lead to two main conclusions. First, the analysis of the actors involved in the development and design of veiliginternetten.nl reveal quite different expectations of the website. This resulted in a rather ambiguous design of the website, and the ambiguous script had subsequently different effects on the real user.

Secondly, I will argue that the envisaged use of the website during design was to a large extent in compliance with the actual use, but without the website facilitating this use. The website, for instance, had no search option, while the actual users expected this option and took efforts to find it. Similarly, that users would look up symptoms and protective measures for particular risks was envisaged as well as enacted, but not included in the description of the various Internet risks. The website was well designed to provide aspects of Internet safety that different Internet users would deem informative, but these aspects were not included in the eventual shape of veiliginternetten.nl.

Table of Contents

1. Introduction

The use of Internet is nowadays common daily life practice in industrialized countries. Most people cannot imagine a life without the virtues and possibilities of internet. But the fast rise and pervasive character of internet also created many debates regarding safety and security issues. With the growth of Internet use, also new risks and dangers came along. Currently, Internet safety is politically and socially an important issue. One of the ways by which governments try to stimulate Internet safety, is to develop user awareness campaigns. However, the effectiveness of these campaigns is questioned (Siponen 2001, Görling 2006). Some studies argue that stimulating user responsibility for overall online safety is a desirable and achievable goal (Stanton 2005, LaRose et.al. 2008). But other studies are more sceptical towards the possibilities to influence user behaviour (Grazioli 2004, Srikwan & Jakobsson 2008) and report that awareness raising tools and other safety tools for end users often lack impact (Furnell et.al. 2008).

Stimulating safe Internet use is thus an important, but difficult to realize task for governmental policy makers. Clearly changing behaviour of end users is a complex issue. Most studies on this problem are either from an engineering point of view (e-security studies) or from a psychological or communication studies point of view. The first type often neglects the human aspect whereas the second type of studies do not question the technology. In this master thesis I aim to contribute towards the understanding of stimulating users towards more safe behaviour from a technology studies perspective. This perspective takes both the technology, the users and their interaction into account. I have analysed in depth the dynamics behind the design and use of an awareness raising tool that was initiated by the Dutch government in 2009, the website *www.veiliginternetten.nl.*

In this introductory chapter I will concisely sketch the development in Internet and the relevance of using Internet in a safe way. Then I will shortly describe the Dutch governmental campaign on safe Internet use, of which I will use the website *www.veiliginternetten.nl* as a case study. This chapter closes with the research question and outline of the report.

1.1 The rise and relevance of Internet

The security issues arising from Internet use have expanded with it's size and use. In its early days, the Internet has not been full of risks and dangers. When the Internet used to be the connected computers from universities to exchange information. Scholars would browse through articles, and click on hyperlinks to continue reading a different article (Nelson 1965). This activity is still well known to us as Internet surfing or: browsing the web. In retrospect this Internet activity was of a static nature. The Internet was a one-way communication channel. The Internet was partly like a television where information was provided through websites rather then television channels (Cormode 2008). Next to the information it provided the Internet also provided simple applications for communication through Bulletin Board Systems and e-mail. And till roughly the mid 1990's, the Internet was not available to many people and had little applications. However, since computers and the Internet have become commercially available and entered the household, the Internet has seen a tremendous growth in it's size: From an estimated sixteen million users in 1995, to two billion in 2011 worldwide (IWS 2011).

With this growth in size, there was also an increase in the application of the Internet. The static Internet became more interactive (Gauntlett 2004; Cormode 2008). People could make comments on products they bought, make profile pages and blogs about their personal lives, hobbies and work. Social Networking Sites emerged where Internet users could stay in touch with their friends and colleagues. Websites using collaborative content creation made their entry. Like Wikipedia for a dictionary, FlickR for picture albums, and del.icio.us for Internet bookmarks. By becoming more interactive, the Internet was no longer made by website designers and creators, but by the Internet users as well. The Internet not only got increasingly more users, the Internet also got increasingly more applications.

In the last years of Internet use, another characteristic of Internet has influenced the way we use the Internet. Internet users can now attribute meaning to (online) data by providing information about the online data. By doing so, websites can now provide data to their users based on the information given to the data by the Internet users (Lassila & Hendler 2007). After the years of the interactive Internet with users generating information, the Internet has now accumulated so much information, that it feeds back information to us on a personal scale. This is seen for example, by advertisements adjusted to your online searching behaviour. The Internet can also suggest books, CDs or movies you might like based on your previous online purchases. Websites can also provide search options that let users browse content based on personal relevance, or based on an attributed meaning like 'interesting', 'biased', or 'funny'. The Internet is no longer a source of information based on computers containing articles which can be browsed through. “The Internet” has now a whole new meaning as if it was an entity where society meets, that knows you personally, and acts accordingly. But the growth of Internet did not grow without it's problems.

1.2 Safe Internet Use

The growth of the Internet, both qualitative (in applications) and quantitative (in users), has given rise to numerous risks and dangers. First computer viruses started to emerge, classified information was retrieved by unauthorized users and computers could even be remotely operated and controlled. And these threats are still with us (Furnell 2010). But the risks for the average Internet user have expanded after they started to supply the Internet with personal information and adopting many of its channels for communication like chatrooms and instant messaging services. Apart from these threats, the amount and nature of the information available on Internet has become so diverse that the term “inappropriate material” now has quite some substance. Like the imagery of child pornography (Quayle 2010) and manuals to conduct terrorism (Wykes & Harcus 2010).

Why these threats are becoming more important and prevalent, is because the Internet is by now not only fully embedded in daily life, but also is an constitutive factor in the shaping of our modern western society. The Dutch government sees the Internet as an irreversible technology[1]. Also my respondents could not image a life without Internet. The owner and CEO of a middle-sized company even stated that the company's daily routine would come to a stand-still if the Internet was unavailable. This thesis asserts that if an important aspect of daily life is prone to responsible behaviour towards it's use, it is important for it's users to be aware of these matters and act so accordingly.

[1] As stated by a clerk of the Ministry of Economic Affairs, during a phone call in 2010.

An important aspect of safe Internet use is the awareness of the risks and the knowledge of the means to act safe. Various websites have been created for the purpose of making users aware of Internet safety. Many governments throughout Europe, large banks and ICT companies, and other organisations have created websites that provide information and guidance on Internet safety. For example the EU website Safer Internet Programme, the safety section on the Dutch banks ING website, and MicroSoft's Safety & Security Centre. Websites on Internet safety are part of awareness raising campaigns, educational efforts and pro-active customer service. And websites are by now a common method to convey knowledge on Internet safety. The Dutch government also created a website as part of an awareness raising campaign on Internet safety. The Ministry of Safety and Justice initiated the Safe Internet Use campaign to raise public awareness on Internet safety and Internet-related crime. The campaign was held in 2009 and 2010. As part of this pro-active campaign, the website *www.veiliginternetten.nl* was created. The Internet has become very important in our society and it is a responsibility of the Ministry of Safety and Justice to lower the amount of (Internet-related) crime. The website veiliginternetten.nl is a good example of a pro-active campaign to raise public awareness of the risks of Internet in society. I use this website as case study to analyse how such a website is designed and used to increase safe Internet use.

There are other reasons why veiliginternetten.nl is a good subject of analysis. It is a relatively large project in terms of the amount of involved organisations, and it is a large website in terms of the amount of possible users of the website (the Dutch Internet users). Using desk research, I found that both the Ministry of Safety and Justice and the Ministry of Economic Affairs, Agriculture and Innovation were involved. And the website veiliginternetten.nl contains a long list of other large organisations in The Netherlands. Examples are tele-communications company KPN, College Bescherming Persoonsgegevens (CBP) and Internet security organisation GovCert. Next to scope of the website, also the available public information is substantial. The website Digivaardig & Digibewust, a website initiated by the Ministry of Economic Affairs, already offers online publications into Internet risks. As projects like these are funded by taxes, much of the information used in the projects is publicly available. Veiliginternetten.nl is thus a website that was created to stimulate user awareness of Internet risks, was created as part of a pro-active campaign to reduce Internet-related crime in The Netherlands, and information about the websites design and use is (at least) partially available for analysis.

1.3 Research Question

In my research I analyse how a website, as a technology, can contribute to the user awareness of safe Internet use. Www.veiliginternetten.nl is used as case study to see how this technology is constructed and how it works.

How does www.veiliginternetten.nl stimulate safe Internet use?

I will elaborate this question from a socio-technical perspective. By using this perspective, I emphasize that the website veiliginternetten.nl is not a neutral tool, but has a certain agency by itself that may influence the user of the website. As will come to the fore in the following chapters, this approach is fairly new in studies that address the problem of the lack of impact of these types of awareness raising tools. Most analyses of safe Internet use campaigns have been from a technical point of view, or assumed the campaigns or websites to be black boxes. By analysing the various actors (both human and non-human) related to the veiliginternetten.nl website, and how they relate with one another, the socio-technical approach can analyse how the website is designed and what the effects are on it's users.

For the analysis of the design and use of the website www.veiliginternetten.nl, I will use the script theory (Akrich 1992). The concept of a script endows artefacts analytically with agency, and enables the researcher to question how the shape and design of a technology contributes to specific problems, in this thesis the problem of changing user behaviour towards more safe Internet use. The core arguments of a script analysis is that during the design, the involved designers make implicit or explicit presuppositions about the envisioned use(r). The actual user however, may 'read' this script in quite different ways. The “misfits” may lead to unintended use that initiators then may label as “ineffectiveness”. This theoretical framing allows me to develop my empirical study in distinct steps. First I will address the question what Internet user was presupposed by the initiators of the website veiliginternetten.nl. Subsequently I'll analyse how this envisaged user was inscribed into the website along with its intended use (the script). Then, I will compare these findings with a selection of actual users and how these actual users use the website, or how they 'read' the script of veiliginternetten.nl.

1.4 Outline of the report

The outline of this report is as following: chapter 2 will give an overview of academic insights into Internet safety and user awareness campaigns. As the Internet is growing and its applications change over time, so do the discussions on the (safe) use of the Internet. “Internet Safety”, both as a concept and what is known about it, is therefore growing and changing. But it's scope is still vague and the chapter outlines some issues that arose in this subject. The chapter then argues that user awareness is a necessary part of Internet safety, and why it's difficult to stimulate.

In chapter 3, I will elaborate the theoretical framework of the script theory. I will enhance the script theory with concepts from domestication theory. From this framework, the website is conceptualized as a technology, and the chapter introduces the vocabulary used to conceptualize Internet users and scripts. Chapter 4 describes and analyses the various actors that were involved in the creation of the website. I will analyse their interests in and perspectives on the website veiliginternetten.nl and how these influenced the actual design of the website.

In the chapters 5 and 6 the analysis is made of the users and the scripts. To analyse this section, research is done into the discrepancies between the user as defined by the creators of the veiliginternetten.nl website and the actual user as established through qualitative research using interviews. Similarly, the intended use of veiliginternetten.nl is compared to the actual use of the website by real users. The discrepancies can reveal the way in which the website relates to users.

In the last chapter 7 I will draw conclusions and give recommendations. The results of this research aim to answer how an informative awareness raising website may contribute to stimulate the users' safe use of the Internet. The insights may contribute to the debate how to design websites that can more effectively contribute to safe Internet use.

2. Internet safety

In this chapter I will elaborate the concept of Internet safety and the academic discussion on the possibilities and limitations of safety awareness campaigns. As Internet develops and changes, so does Internet safety. Although awareness campaigns to stimulate safe Internet use are relatively new, they have been studied and evaluated by several scholars. Based on the discussion of these studies, I will position the relevance of my socio-technical approach of analysing safety awareness technologies.

2.1 A virtual world of dangers

In this section I will try to outline the scope and content of Internet safety. If we are to stimulate safe Internet use, then what do we refer to when discussing Internet safety? What risks and dangers are we to be aware of? The concept of Internet safety is widely used by scholars as well as policy makers. However, a stabilized definition of the concept is lacking, and quite some similar concepts circulate.

In current literature one can find various general descriptions, e.g. "*vulnerability and exposure to dangers - knowingly or unknowingly – when using Internet and other digital technologies*" (Cranmer et.al. 2009, p128), but there is not yet a stablized definition of the concept of Internet safety. Also notions circulate like *information security* (Solms, R. von 1999), *e-safety* (Sharples et.al. 2008), *Internet security* (Siponen 2001), *computer security* (Stanton J.M. et.al. 2005) and *iSafety* (LaRose et.al. 2008). For practical reasons, I use the notion of 'Internet safety'.

To understand the concept of Internet safety it is more fruitful to look at what it contains, rather then find out how it is defined. The risks and dangers of computer- and Internet use are reported extensively. For example, one study analysed the failure to detect deception on the Internet (Grazioli 2004). Internet deception and fraud were conceptualized into page-jacking and test subjects were tested against this particular Internet threat. A broader collection of Internet risks was used to research the security advice from ISPs and retailers: Adware, Identity theft, Phishing, Spam, Spyware and Viruses are what the researchers used as Internet risks (Furnell et.al. 2008). An even broader range of Internet risks is found in the UK government's categorization of e-safety risks and dangers centred around four C's: content, contact, commerce and culture. 'Content' includes inaccurate or misleading information and illegal material (e.g. of child abuse), 'contact' contains grooming via communication programs (Skype, MSN, chatrooms), 'commerce' includes online gambling services and 'culture' names bullying and downloading copyrighted material (Cranmer et.al. 2009). The inventory of risks and dangers of computer- and Internet use is very extensive.

Many Internet risks and dangers overlap with already existing and known non-digital forms of crime. With a risk like 'theft' we both mean that one could lose their wallet on the street, or loose private documents on Internet applications. Can we distinguish between the two? Because the words 'Internet safety' indicate that whatever is unsafe about the Internet and it's use thereof, it is differently unsafe from what we normally (outside computer- or Internet use) deem unsafe. What is unsafe about the Internet according to David Platt, professor of software engineering, is that "*bad guys in cyberspace want to harm you ... through running programs on your computer, or stealing your sensitive data, or some combination of the two*." (Platt 2007, p68). A computer virus is then a prime example of Internet safety. It is a computer program that 'infects' a computer by destroying or distorting information on that computer, and can spread itself by making copies of itself and sending it to other computers connected to the 'host' computer. A computer virus can exist only on a computer, and spreads itself through the connected computers: cyberspace. For Platt, Internet safety thus deals with those risks and dangers that limit itself to computers and the communication between them.

But there are two problems with definitions or taxonomies like these. First, it excludes risks and dangers which we only attribute to Internet use (like online bullying) which do not rely on programs being run or stealing sensitive information. Just like phishing e-mails, grooming and gambling websites. Secondly, as Platt points out ironically, there is a big difference between someone trying to steal your car, which takes time and one car somewhere close to the thief, and someone trying to steal passwords via tens of thousands of computers worldwide. At once. Continuously. There is a virtual world of dangers, but is hard to find the exact nature. And with risks like theft the scope becomes very vague.

A similar case was made in an article about Internet deception (Grazioli 2004), arguing that "*deception and fraud are not new phenomena, [but] it is argued that the specific characteristics of Internet Technology have changed some of the conditions under which these malicious practices are carried out, and as a result have introduced new elements, worthy of fresh scientific study*." (Grazioli 2004, p.149) Here, Grazioli and Platt have very similar reasons. Both point out that Internet has done away with distance, and that it is made much easier to commit crimes faster (more harm done per time segment). Platt adds that the tools to do so are much easier spread around the world, but Grazioli brings forth much bigger problems concerning the Internet. Namely that it is very difficult to verify the identity of the involved people. Even if this is done, legal prosecution is very difficult because there either aren't laws to pursue these people, or they are incompatible between countries.

So the concept of 'Internet safety' indeed refers to distinct phenomena than general safety. A virtual world of dangers emerges when using computers and the Internet. It is important for Internet users to be aware these risks and dangers. And it is important for society as a whole. A good number of risks have been identified and conceptualized, and known safety issues like theft are taking on new forms. That there is a need to be aware of these risks and dangers is reflected in the emergence of safe Internet use campaigns. The Internet is used by over two billion users and as a technology embedded in daily life. To create effective campaigns to stimulate a safe Internet use, however, is not an easy task, as the next section 2.2 will show.

2.2 The necessity and difficulties of user awareness

There are good grounds why user awareness towards Internet safety is necessary. Here I provide two reasons why stimulating user awareness on Internet dangers is important and necessary. First, the use of Internet is by now embedded in daily life. The Dutch government sees Internet as an irreversible technology, and digital literacy is seen as a requirement to fully participate in our (current) information society. The Ministry of Economic Affairs therefore initiated the pro-active campaign Digivaardig & Digibewust to stimulate the digital literacy of the Dutch citizens. However, they too anticipated the necessity to make users aware of the risks involved with Internet use. The website veiliginternetten.nl this became linked to this Internet enhancement campaign. Not just for The Netherlands, the Europe Union has launched a similar project, including websites like veiliginternetten.nl.

Apart from this societal reason, there is another reason why user awareness is important. There are no technological fixes that guarantee the safe use of the Internet. To explain this, I'll use traffic safety as an analogy to Internet safety in terms of it's technical aspect and one's responsibility. By now traffic safety has seen various technologies to stimulate safety. Seat belts are one, the “anti-blokkeer-systeem” (ABS), various signals, speed bumps. A person in traffic has various means to enhance personal safety, as well as being guided by other means to further this cause. However, as any driver knows, there is no *guarantee*. One must still be aware if another car pays attention and sticks to the rules as well. Whether or not that pedestrian wants to cross the road suddenly, or paying attention to your velocity to shorten breaking distances. It are these dangers that cannot be prevented by any technological means. One must be aware in traffic. As for Internet. There are no technological methods available that would guarantee safe Internet use, or: technological fixes to stimulate Internet safety only get us that far, it needs to be complemented with one's own responsibility to act in such a manner.

Thus stimulating users to take their responsibility of using Internet in a safe way is a necessary element of policies stimulating Internet safety. To prevent the average Internet users from unnecessary harm, user campaigns have been initiated. Most campaigns address two aspects. The first one is to raise the awareness that these risks is desired. An example of the first aspect is stimulating the awareness how easily a password can be guessed. Short passwords for example, can easily be guessed. Just like passwords that are the name of your spouse, child, or pet. The second aspect is to provide concrete methods and tools that aim to stimulate more safe Internet use in practice. Examples are practices like changing passwords regularly or using a firewall. Another example to stimulate safe Internet use, is using a virus scanner that can detect harmful programs and remove or isolate them.

Making the Internet users more aware of risks and providing tools for safe Internet use are currently important ways in which users are to be kept from harm when using the Internet. The are both desirable, but also hard to realise. In the literature we can find studies that report successful awareness campaigns, however other studies are rather sceptical about the effectiveness of stimulating safe Internet use. Below I will describe and discuss both points of view and position my own approach.

Different points of views on the (in) ability to raise user awareness and change user behaviour.

Several studies report that user awareness campaigns can be successful in steering safe online behaviour. LaRose et.al. (2008) study on promoting personal responsibility for Internet safety using websites, shows that it works. They have analysed different methods from ten websites and their effectiveness on safe Internet behaviour. They distinct eleven methods to stimulate safe behaviour, varying from raising awareness of the risks to the strength of habits stimulating safe Internet use. These methods were derived from key concepts used in psychology studies. They conclude that "*the average user can be induced to take a more active role in online safety. Progress has been made in uncovering the "pressure points" for effective user education*." (LaRose et.al. 2008, p76) All ten websites that were analysed were specifically designed as online safety website. These websites were commissioned by organisations like the U.S. Department of Justice, the U.K. Government and the Internet Education Foundation. Based on individual online protection and people's attitude towards it (research of its social dimension) the analysis of the websites and their effectiveness did show an overall increase in personal responsibility. "*Thus, improvising user responsibility for overall online safety is a desirable and achievable goal*." (Ibid, p76).

Stanton et.al. (2005) too analysed end user security behaviour. Whereas LaRose et.al. used methods to stimulate safe behaviour based on psychological knowledge, Stanton et.al. developed a scale of security behaviour based on over a hundred interviews with ICT security professionals. The scale makes a distinction between both the computer expertise needed to perform certain actions, and the intention of the action. The intentions could be malicious or benevolent. The resulting two-factor taxonomy suggests that safe Internet behaviour becomes risky when Internet behaviour resembles "dangerous tinkering" or "naïve mistakes" (Stanton et.al. 2005, p127). Subsequently, they analysed how organisations and their personnels safe Internet use could 'climb up' this scale of security behaviour. They conclude that "*several mechanisms may help to move end user behaviour from the naïve mistakes category to the basic hygiene category*". (Ibid, p131) The names given to different security behaviours, it means that mechanics can steer Internet users towards more secure behaviour. In addition, their taxonomy "*suggests paths that an organization can take towards improving its security status*". (Ibid, p132)

Clearly, current academic literature shows that increasing user awareness on Internet safety is, at least targeted carefully, desirable and attainable. However, other studies are much more sceptical about the effectiveness of measures to stimulate safe user behaviour. As desirable and necessary user awareness may sound, research done into its effectiveness forms a grim picture. From human psychology to the awareness campaigns currently at hand, user awareness has a long way to go before it's on par with it's premises to do so. Below I will discuss some studies that argue why it is so difficult.

A striking paper was published for the Virus Bulletin Conference called "The Myth of User Education" (Görling 2006). In this paper Görling described an extensice list of literature in which user education towards safe Internet behaviour has failed. His conclusion is that "*computer security experts must cease to consider themselves as a theoretical sub-field of computer science, but rather expand and borrow knowledge from various disciplines, including behavioural fields such as Human Computer Interaction, and abroad range of other disciplines which may help to put security back into context, such as the fields of organization theory*". (Görling 2006, p3) These words resonate something written 5 years earlier, namely that "*The concept of awareness may have been not considered in greater depth because it falls outside the scope of the traditional engineering and "hard" computer sciences*" (Siponen 2001, p24). A first difficulty facing Internet safety is its vague scope and overlap with other fields of science.

A second difficulty is a false sense of security. For example: People who have virus scanners impose a greater threat to security because they *think* they are safe and can therefore click on anything that appears on their screen (Görling 2006). The notion of a false sense of security is point of departure for Srikwan and Jakobsson (2008), who analysed how cartoons could stimulate Internet security, and write that "*it is not surprising that the average consumer has a rudimentary understanding of the threat, [...] To make it worse, phishing is both a matter of technology and psychology, and there is ample evidence supporting that most people* want *to trust what they see.*" (Srikwan and Jakobsson 2008, p138)

A similar difficulty is found in the overlap of Internet safety with psychology. Grazioli (2004) tested consumers' abilities to detect deception over the Internet. They even used "IT-savvy" Internet consumers and tested them against page-jacking, a practice very similar to phishing. Conclusions were that "*although a few succeeded, overall these subjects were* unable *to detect the deception*". (Grazioli 2004, p168) Görling referenced similar research and quoted an article called "Why phishing works" in which 40% of the test subjects fell prone to the deceptive practice. To better understand how users can be educated in Internet safety, computer science does indeed not cover all aspects.

Another inability to make users aware is found in the works of Furnell (2008). The means to educate the user are not always well "designed". He investigated the security advice and guidance from retailers and ISPs towards Internet consumers and wrote that "*while the need for end user education is often acknowledged, our research has highlighted the lack of impact of existing efforts*" (Furnell 2008, p9). Internet safety was conceptualized into adware, identity theft, phishing, spam, spyware and viruses. And the means to educate the Internet users was the advice of above mentioned vendors (in the UK). During research some involved respondents failed to mention that their companies had websites with relevant information about Internet security. Meanwhile, "*it would be desirable for stores to have at least one security-aware advisor who could be called upon to meaningfully explain the threats to customers and advise them on protection.*" (Furnell 2008, p9) If the means to stimulate safe Internet use are not well designed (like giving wrong advice or not redirecting to more useful resources), they don't function well.

Achieving user awareness towards safe Internet use thus is a complex and difficult task. Literature shows an ambivalent picture. On the one hand there is a strong case to make that user awareness is desired if not necessary to have towards Internet safety. On the other hand, most of the efforts to do so are ineffective. In short: we need to make the user aware of the risks and dangers of Internet, but its difficult to realize. Perhaps, the lack of success is because it is not taken as a new discipline (Siponen 2001, Görling 2006). Most studies are limited to either an engineering or a psychological perspective. To continue to the ongoing research my thesis adds a science and technology studies perspective in which technologies, in this case websites, play an important role in shaping human action.

3. Theoretical framework and methodology

This chapter outlines the theoretical framework for my research. I will apply a Science & Technology Studies (STS) point of view that allows for an in-depth look how these technologies are designed and how they interact with their users (Latour 1992, Akrich 1992). By adopting this view, the website is understood as emerging from a group of people, organizations and (sub-)technologies. Together this group creates, designs and shapes the website. The result of this is analysed by using a script analysis (Akrich 1992). Scripts are, simply put, ways in which the technology at hand is assumed to be used by it's designers. The discrepancies between designers' scripts (how they think it will be used) and how it's actually used is central to script analysis. This chapter first will describe the script concept, then I will elaborate the framework for comparing the inscribed user and the actual user. This chapter closes with a methodological section.

3.1 Script analysis

How was veiliginternetten.nl intended to be used? In what way was this intended use materialized into the website? How did real users subsequently use the website? To answer these questions a script analysis is done. This section outlines the theoretical framework of the script concept and describes how the script concept is used in the analysis of the website veiliginternetten.nl.

Once an actor or a group of actors starts creating a new technology, the involved actors too begin to assume and presuppose certain actions by the envisioned users. Also a process of delegation begins, where some competences and responsibilities of humans are delegated to technical objects. A technology like veiliginternetten.nl will hence have not only certain characteristics and an envisaged use towards it's constructed user, it will even be given competences and responsibilities. The inscription of this envisaged use along with delegated competences into the new product, is called the 'script' of a technological object by Akrich (1992, p207-8):

> "*Designers thus define actors with specific tastes, competences, motives, aspirations, political prejudices, and the rest, and they assume that morality, technology, science, and economy will evolve in particular ways. Alarge part of the work of innovators is that of "inscribing" this vision of (or prediction about) the world in the technical content of the new object. I will call the end product of this work a "script" or a "scenario*".

The script of veiliginternetten.nl, then, contains inscriptions regarding the characteristics of the potential users as well as materially encoded prescriptions regarding the behaviour of the user. The desirable setting for veiliginternetten.nl and distributed roles between the artefact and the (constructed) user is encoded in the website. Veiliginternetten.nl's script is the totality of inscriptions, prescriptions, distribution of competences and responsibilities as designed by the group that created the website.

Jelsma (2006) has applied the concept of script to study the potentiality of a technology designed to change behaviour. In his research, he looked how a product could be designed in such a way that it induces a desirable change in behaviour of it's users. In his paper he analyses how the design of a dishwasher may influence the user behaviour towards more energy efficiency. This is what Jelsma calls the design of "moralized" products. This makes for a very comparable case to veiliginternetten.nl as the intention of the website aims to change users' behaviour in more safe Internet use. In both cases, the dishwasher and veiliginternetten.nl, these behavioural changes are endorsed by the government, and even the slogans for these two campaigns are alike: For energy saving the slogan "A better environment starts with yourself" was used, and for safe Internet use the slogan "Safe Internet use is in your own hands" is used.

Jelsma (2006) has developed a schematic overview of the various parts of a script analysis schematically (see fig. 1). In the area above the grey horizontal line, the designer (or creator) of a technology has a fictive user in mind (the constructed user) and inscribes the assumptions about this user into the design, the script of a technological artefact. When the artefact is used in actual use situations, the real users " de-inscribe" or "read" this script.

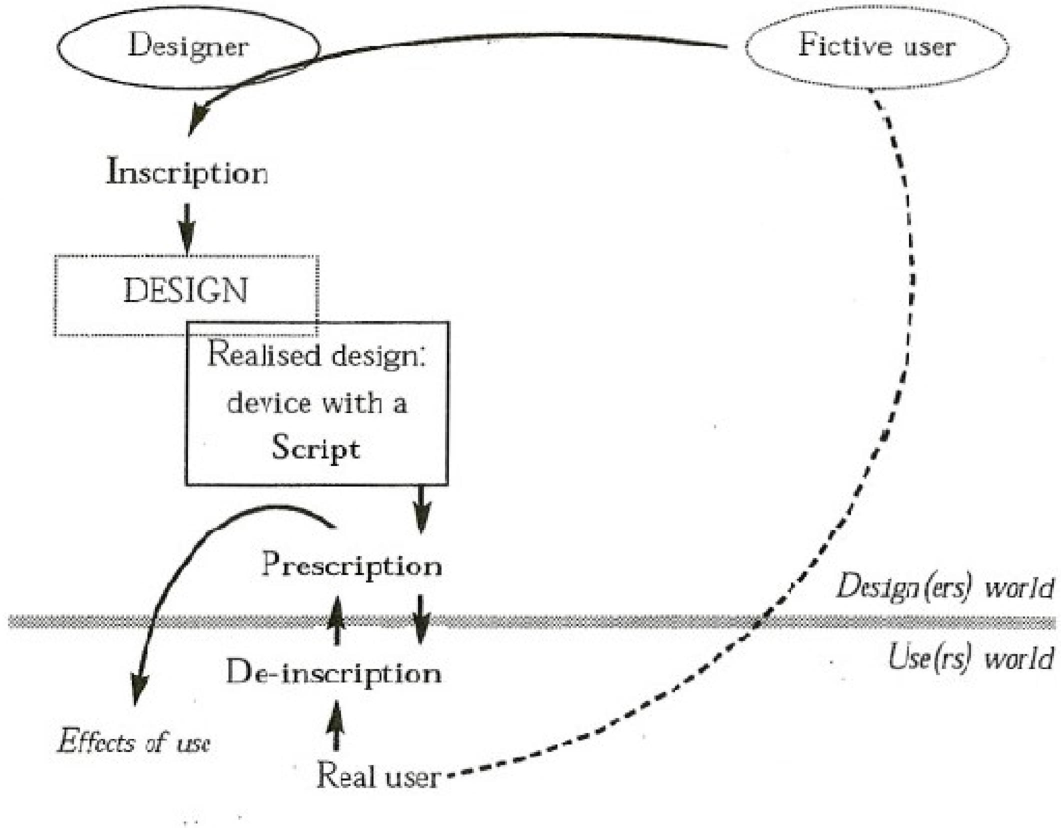


Fig. 1: The concepts of design and use processes schematized (Source: Jelsma 2006, p224).

Jelsma has developed two useful notions for analysing the relation between design and use of artefacts: *script logic* and *user logic*. Script logic refers to the script of the device as inscribed by the designers. But as STS research has shown, users do not always follow this script and "*actively domesticate novel artefacts, instead of just following unequivocal messages from scripts in one inescapable way*" (Jelsma 2006, p225). Script logic hence refers to the script prescribing a use as envisaged by the designers, and user logic refers to the de-inscription as done by the real users. Both logics influence the actual impact of use on pursued changes in behaviour, in my case, safe(r) Internet use.

To complement the vocabulary on script analysis, I will adopt the concepts of *invitation* and *inhibition* as introduced by Verbeek (2005). With these terms he refers to acts that are stimulated or discouraged by the design and shape of the artefact (Verbeek 2005, p171). These concepts are illustrated by the often used example of the hotel keys from Bruno Latour (1992). As hotel managers want their tenants to hand in the keys to their hotel rooms upon leaving the hotel, they attach a heavy or otherwise cumbersome object to the key. The attachment to the key *invites* the behaviour to hand it in, and *inhibits* the act of putting it in any of your pockets.

With the notions of invitation and inhibition, it is now possible to describe prescriptive effects the veiliginternetten.nl website can have on it's users through its script logic. And I can now describe the 'effects of use' through analysing the real of use of veiliginternetten.nl and user logic. My research analyses what was inscribed by the designers, it analyses the script from the device, and the de-inscription by the users. The first two are found above the grey horizontal line in the schema, in the designer world. The third analysis is found in the user world.

Script analysis has been applied to various technologies since it's introduction. Usually, these technologies are concrete material objects, like the dishwasher in Jelsma's (2006) analysis. Yet applying script analysis to a non-material artefact like a website is not new. Oudshoorn and Somers (2006) and Rommes (1999, 2002) have done so respectively with websites for patient organisations and for Amsterdam's De Digitale Stad (DDS). Oudshoorn & Somers have studied how user representations of patients were inscribed into the design of the websites of three patient organisations. The website users thus are patients who suffer from illnesses that may affect their approach to websites. For example, they may have short attention spans or an inability to perform many actions with their mouse. Oudshoorn & Somers analysed how the websites were 'custom made' to accommodate the specific characteristics of their future users.

Also Rommes (2002) performed a script analysis of a website. She studied one of the first municipal websites to inform and involve citizens, Amsterdam DDS (De Digitale Stad). DDS was a website that was to provide a virtual version of the city. Being quite extensive, a user of the website had a good amount of options (uses) at their disposal to engage with the website. Rommes analysed how first time users would engage with the website, something found in my research as well. How I differ in approach is that her script analysis was done into the website to see how people would use that same website, rather then analysing if people's behaviour was changed. As her research is from a period in time where computer- and Internet use was fairly uncommon in society, her first time users also include people who had not used a computer before. In my case study, the users of the website veiliginternetten.nl, both the represented user as well is the actual user, all will have Internet skills. The level of skills, however, can vary greatly. As the target group of veiliginternetten.nl encompasses all Internet users in the Netherlands, my case study, thus involves a situation of "configuring the user as everybody" (Oudshoorn et.al 2004). In analysing these type of technologies, Oudshoorn et.al (2004) strongly emphasize the relevance of taking account of user diversity, both for designers but also for the script analysis. I will therefore in my empirical study also explicitly aim at the analysis of a diverse group of users.

To summarize, by applying a script analysis I will thus first describe the process of inscribing "the constructed user" into the site veiliginternetten.nl. To do so, I will map the involved stakeholders in the design process. Secondly, I will analyse the script of the website itself by describing its inviting and inhibiting elements. Thirdly, I will analyse the process of de-scription of veiliginternetten.nl in its actual use by a small, but diverse group of users. In the next section, I will zoom into the dynamics of constructing a representation of the envisioned user.

3.2 The constructed user and real user

When developing a new technology, also the use practices of that technology are more or less explicitly considered. Before the technology is designed, a future user is envisioned, with certain knowledge, skills, interests, habits, etc.. Designers often construct a future user to create a technology that is fit for those particular users. One would not make a technology for, say, the blind that requires them to read a display from a device. But in some cases it is hard to grasp what the future user will be like when introducing a technology that targets almost everybody. How does one construct an image of a user for a website that is publicly accessible for all Internet users and stimulates them in safe online behaviour? How does one construct an Internet user that is prone to cybercrime?

This section introduces the means and vocabulary to make an analysis of the future user and real user. By comparing them, an analysis can be made if there is a mismatch between the envisaged user and the actual user of the websites. Any discrepancies with the envisaged users can reveal if real users use the website as designed. And by interviewing the real users before and after the use of the website, discrepancies between those moments in time can reveal a different behaviour towards safe Internet use. First I will introduce ways designers use to create a picture of a future user, then I will introduce a model to describe an Internet user that is prone to cybercrime.

User Representation Techniques

Akrich (1995) has described six methods in which a representation of the future user can be constructed. These are divided into explicit and implicit techniques. The explicit techniques encompass the construction of a user based on the interpretation of data provided by the users themselves, and implicit techniques rely on the statements of others about the users. So when a technology is created that constructs a future user, explicit techniques look directly at the users, while implicit techniques are based on indirect methods.

Explicit techniques include market surveys, consumer testing and feedback on experience. In these three techniques the users make statements about their experience with the technology. Respectively by using questionnaires or interviews, by letting users test the technology in a controlled environment, and by letting users give feedback after using the technology at their own discretion. Implicit techniques include “I... methodology”, “The experts”, and “Other products”. These somewhat more vaguely named techniques refer respectively to: Designers placing themselves into the position of the user (think and act like them), people who can speak on behalf of the user through knowledge and experience with the user, and user representations from similar technologies.

In practice, not all these techniques are, or should, be employed when constructing an image from the user of a technology. As chapter five will show this has also not been the case for the veiliginternetten.nl website. I will analyse which user representations were inscribed, and how they were constructed by using the methods named by Akrich. To subsequently analyse those representations, and the data of my own interviews with real users, I will use a model from Punie (2000). In this model he combined multiple methods of analysing the real users of technologies.

The Real Users of veiliginternetten.nl

In domestication theory, there are three stages for new technologies: A technology is created with a particular use and user in mind (commodification), the technology is subsequently used in the household (appropriation) and it's experiences and uses feed back into the technology (conversion). Already in the chapter outlining the domestication theory, the authors dedicate a good deal on “constructing the user” (Silverstone & Haddon 1996). The theory of domestication has already been widely adopted by scholars, specifically towards information and communication technologies (ICTs). Out of the research, both quantitatively and qualitative, Punie (2000) has constructed a model that shows the different factors that come into play when analysing the actual use of ICT. (See fig.2)

The grey area indicates the phase of appropriation. Where users have obtained the technology and apply it in their home. The three factors left of the grey box (attitude, knowledge & capabilities and time-space) are dominant factors in describing users and as will follow in Chapter 5, had similarities with the research into the future user by the designer. I will use this model to describe the constructed user, the Internet user prone to cybercrime. The model includes a section for the socio-structural position, as well as on the right side 'ICT ownership' and 'ICT Usage', but I only use this model to describe a user with the three characteristics left of the grey box. Unlike Punie’ s study that elaborates primarily the ICT use (domestication), my study focuses on the design-use interface.

The attitude of users, the first characteristic, is how users think about a technology. This not only includes how people personally feel about a technology, it also includes reigning paradigms and culture. That it is rude not to answer your telephone, or neglecting not to reply to e-mails quickly, are examples of a technological culture.

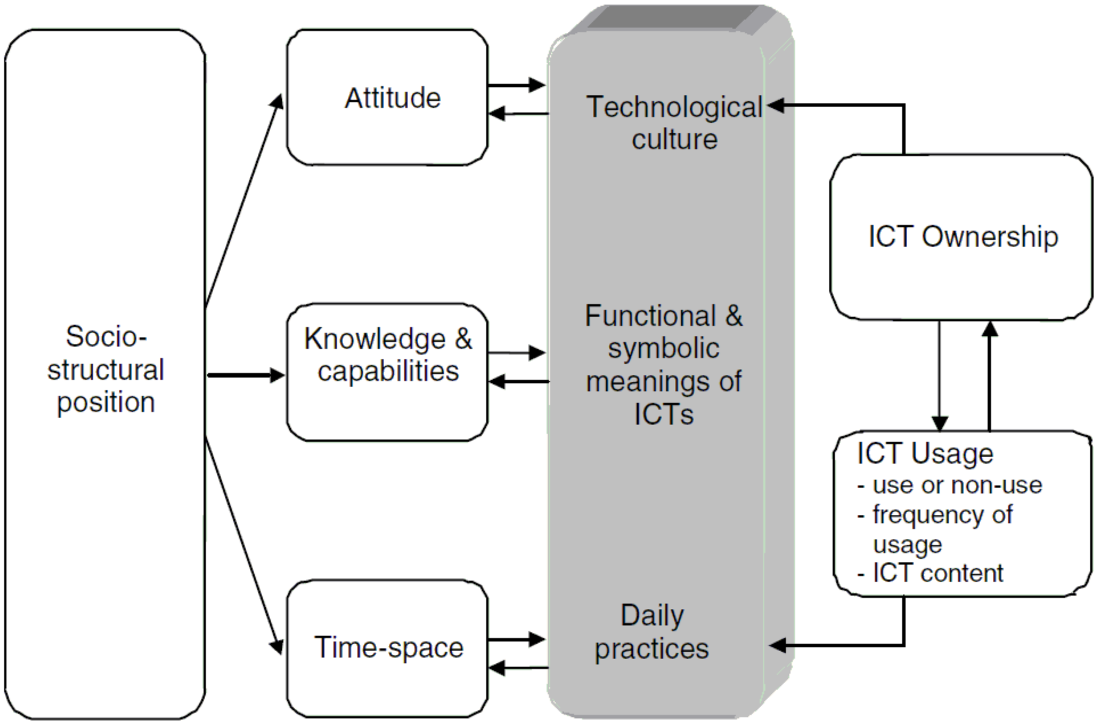


Figure 2. A model for ICT domestication. (Source: Punie 2000)

The factor of knowledge and capabilities can roughly be taken literally. What people know about a technology, how to use the artefact (if it has one), what the technology is for, for whom it is intended, are examples of a person's knowledge and capabilities towards a technology. Time and space, how abstract it may sound, simply refers to the daily practices. Where does the technology find itself, usually physically, in your household? How many times do you use it? The concrete picture how people give a technology a place in their daily routines make up for the third factor in describing a user of a technology.

With the techniques described by Akrich and the model for the dimensions of ICT use from Punie I can now investigate the real user and analyse the user representation techniques of the inscribed user. This allows me to make a comparison between the constructed user and real user. And with these findings I can analyse the design and use of the veiliginternetten.nl website within my semiotic framework. To see if, and how, the website stimulates safe Internet use.

3.3 Methodology

To answer the research questions, I approached and interviewed the designers of the campaign and I selected a small sample of users and interviewed them on their experiences with the use of the website (see 8.3 Interviews). The designers were interviewed to gain information for the analysis of the user representations and inscription process. The designers too provided me with the core documents that were written and used during the construction of the website I selected four, diverse Internet users who were not acquainted with veiliginternetten.nl. I conducted qualitative interviews with these users twice, once before and one after they visited the site veiliginternetten.nl. This allowed me to describe a picture of the real users and how they de-inscribed the website.

Performing a script analysis

To start the analysis of the design, I will make a reconstruction of the actors involved in the design of veiliginternetten.nl. For this, I held an interview with the campaign manager and her online consultant and analysed briefings that were used during the creation of veiliginternetten.nl. As described in chapter four, the actual construction of the website was not done by just one actor. One actor that acts as "*director of the campaign*" (Interview de Jong, campaign manager, 2011), delegated the creation of the website to an online design company, who in turn delegated the creation of the individual web pages to an IT company. The goals of the campaign were passed onto the various parties using briefings. These documents contain descriptions of how the website is to be constructed. Among these descriptions are it's goals, aims, messages, content and tone.

Secondly, the script analysis of the website was done by visiting the website and describing it's content. How is the website constructed and what can be done with the website? To describe the script the website is taken as a technological artefact and it's different uses and functionality is put into words. By doing the script analysis of the website I had to take two things into account. The first is that I could fall prone to an approach to the website from my own vision of the world. One that is very technical of nature and mostly shared with the designers. This problem was already stated in the research of Rommes et.al (1999), who adopted the perspective of 'outsiders' to counter this situation. A solution I will adopt as well. Furthermore, during the two year campaign the website has changed in appearance. I used the latter website, the one that saw a revision after the first year in which the campaign had run it's course, because this version was used by the people I selected for my research.

To analyse the user representations, I had to obtain information that was used to make assumptions about the Internet use of the future users. As the campaign had run it's course and the actual user was known to the manager, I used as primary source not the interview with the campaign manager, but the research reports of the quantitative and qualitative surveys that were executed prior to the campaign. This was both quantitative as well as qualitative, and encompassed respectively 600 and 20 respondents. This enabled an analysis of the construction of the future user.

Selecting the real users

To find users of veiliginternetten.nl within the large target audience (the Dutch public) I chose people within my personal circle. As they could have been already informed on the subject matter, I asked preliminary questions regarding their knowledge and experience with ICT security and their familiarity with the government campaign. The criteria I applied were: No specific knowledge of ICT through personal education, interest or work; Using Internet in daily life for personal matters; No prior subjection to campaigns or courses that stimulate safe Internet use. By applying these criteria, the users would be average Internet users who could be stimulated by informative means.

Within this subgroup of my personal circle, I continued to select users to include a diversity of personal characteristics of Internet users. For this I used the classifications of ECP-EPN. This large ambitious project issued by the Ministry of Economic Affairs aims to educate the Dutch public on computer- and Internet use, and divided the Internet users into four categories: entrepreneurs, parents & children, the elderly, and digital illiterates. To further broaden the range of characteristics, I took users with different ages, genders and occupations. The youngest user was 30, the eldest 79. Three are female, one is male. As I use a qualitative approach to create a picture of the real user and the real use of the website, these characteristics of the users allow for a broad exploration of the reasons why and how they adopt safe Internet use practices. Based on my own criteria, complemented by the ECP-EPN classifications, the following four Internet users were chosen to participate in the research:

> Jan van Kranenburg, a middle-aged entrepreneur. After successfully creating and selling his former company, he has now started his second company along with a partner. The new company centres on polymer research, and holds a staff of roughly fifteen members. The company is situated in Deventer and I approached Jan as the entrepreneurial Internet user.

> Ilona Wiltink, a thirty year old mother of a baby boy. She works in a health care organisation by day, and vividly uses Internet in the evening at home. With her son rapidly growing to the age of Internet use, Ilona is paying attention to this event, and is determined to have her son engage with the Internet in a safe manner.

> Wil Klosters, a 79 year old woman who has seen Internet arrive in her life, and now uses it for e-mail and to have occasional conversations with her family in Canada using Skype. Although she was a little sceptical if she could be a possible candidate for Internet research, I explained how such deviating approach to Internet could reveal interesting insights into the current Internet user. And she agreed to participate.

> Marije van Kuijk, a 37 year old married woman. She works as an optician at an optician's store in Deventer. Although she uses internet, like Ilona, mostly at home, she also uses computers for her work. After a conversation about the computers and software that her store used, I mentioned that user feedback was very useful in the design of software, and asked her if she would contribute to such research. Although Marije is not chosen from my personal circle, I did apply the criteria mentioned above. She has no particular work in ICTs, uses Internet daily, and can't remember to have seen a user awareness campaign about Internet use. I chose Marije for the last classification from ECP-EPN. The latter classification, called somewhat belittling 'the digital illiterates', I behold to refer to the average Internet user. One that does use internet, but has no particular education in- or knowledge of ICTs, and uses Internet for it's possibilities, comfort and leisure.

I conducted two qualitative interviews with each user. The first was to create a picture of them as Internet user and their attitude and knowledge of cybercrime. The second was to create a picture how they used the veiliginternetten.nl website. When asking them for the interviews, I had them choose a location at their own discretion, and asked for a maximum of one hour to ask my questions. Two of them choose their own home outside working hours, the other two had the interviews being conducted at their work as they preferred that. There was roughly a week between the interviews with each user, the time I gave them to use the veiliginternetten.nl website.

The first interviews were semi-standardized and took on average 45 minutes. In these interviews, I asked them about their Internet use and attitude towards cybercrime to describe them as real user. At the end of this first interview, I asked them to look up the veiliginternetten.nl website and use it to stimulate their online safety. As I assumed this would not make up their agenda for the entire week, I asked them to make a few notes when using the website as reminder to them for the second interview. Three of them made notes and brought them to the second interview. With roughly 25 minute interviews, I formed a picture of how they approached and used the website.

With Jan, Wil, Ilona and Marije, I have a group of four distinct Internet users. With different approaches to internet, different occupations, genders and situations in life. This makes up for a broad range of different Internet uses. By choosing a group as based on the categorizations from the ECP-EPN project, I opened various approaches one could have towards the website. This allows me to create a broad and detailed picture of the various stances towards cybercrime as adopted in the real user. And similarly for the use of the veiliginternetten.nl website. With a science & technologies studies point of view, it are these broad and diverse pictures that further our understanding what happens between a technology and their users.

The limited number of four Internet user is also the result of restricted time to conduct the project. Two users per ECP-EPN category could have been used, or the categories could have been expanded. But in the time and means available, the picture of the real user and actual use of veiliginternetten.nl will be created using four individuals. The limited time too is reflected in the number of interviews with the stakeholders in the design phase of the website. Only the most central actor who had the responsibility for coordinating the project was interviewed, together with her online advisor. However, combined with the document analysis the empirical data was sufficient to analyse the design dynamics and the positions of the various involved stakeholders. The available data allowed me to reconstruct quite an extensive network of involved stakeholders.

In the next chapter, the first empirical chapter, I will sketch this network of stakeholders and the world of meanings from which the actual website veiliginternetten.nl emerged.

4. Mapping the design context of veiliginternetten.nl

In this chapter I will analyse the group of actors that was involved in the construction and design of the veiliginternetten.nl website. By mapping this network, I can give a picture of the different actors that have an influence on the website's eventual shape and intended use. First I will give an overview of the time before the website was made public. During this time the website changed in appearance once. This was after the central topic of the campaign changed. Then I'll introduce the different actors. The mapping of this group of actors, including an additional look at online means to stimulate user awareness, will reveal rather different actor perspectives on the goal, intention and shape of the website. Differences that too will have their effects on the design and script of veiliginternetten.nl.

4.1. Overview of the development of veiliginternetten.nl

In 2008 the Ministry of Safety and Justice decided to start a campaign to make the public aware of the risks and dangers of internet. This ministry is the funder as well as the commissioner of the campaign. The execution of the project was given to the communication department at the Ministry of General Affairs, called Dienst Publiek en Communicatie (DPC). This department is also responsible for general informative campaigns of the government, known as "Postbus 51". Campaigns under the name of Postbus 51 are well known with the Dutch public to be "information from the government", which is also Postbus 51's slogan. DPC in turn, is by now well experienced with executing these campaigns.

As the website is part of a campaign created by DPC, this communication department became the central actor. They started with the commission of qualitative and quantitative research into the practices of Internet use and the attitudes of Internet users towards Internet risks. This research was executed by external research bureaus. The information from these surveys was combined with the commissioner's goal to create briefings. Briefings are roughly plans of action on how to construct the TV commercials, websites and other products that shape the campaign. These briefings were subsequently sent to the marketing- and online bureaus that would build the products. While these different actors all became part of veiliginternetten.nl, DPC maintained communications with their commissioner and firmly rooted itself as the centre of the network. "*We hold the ropes to all different parties that have a role in such a large campaign*." (Interview de Jong, campaign manager, 2011).

The products that followed we're not used throughout the 2 year campaign. After the first year the central topic of the campaign shifted from 'online personal information' to 'identity fraud'. Because this encompassed financial transactions and misuse of online identities, the Ministry of Economic Affairs gained an interest into the campaign. "*Economic Affairs had a stake in the campaign because it's their task to guide the people in the market and to conduct trade well.*" (Interview de Jong, campaign manager, 2011). This also meant that an emphasis was placed on different Internet risks, with accordingly different information and tools to inform the people.

The Ministry of Economic Affairs also became involved, approximately a year after the start of the project. This department was already involved in a project called Digivaardig & Digibewust (roughly translated as Digi-literate and Digi-aware). This substantial and large project involving government, corporations and social enterprises has different sub projects to educate "*all (Dutch citizens) to be part of the digital development*", because "*in a few years, digital literacy is as important as learning to read and write*". (Digivaardig & Digibewust website 2011) Learning the risks and dangers associated with this new digital development is quite useful in educating the public. And the safe Internet use campaign from DPC was just one among many of the efforts in the Digivaardig & Digibewust campaign to educate the Dutch citizen in general computer and Internet use.

Initially, the core actors wanted to involve much more different actor into the Internet safety campaign. In the first meetings of The Ministry of Justice and DPC it was thoroughly discussed to incorporate companies, stores and (supply chain) vendors into the project. To provide protective means more cheaply for example. However, The Ministry of Justice argued that it would not be feasible to include the affected parties in it's entirety, and the idea was abandoned. Still, efforts were made to include as many partners as time and means would allow to give the campaign more momentum. Like the largest tele-communications company in The Netherlands (KPN) devoting an article to it in it's monthly newsletter. These activities however, were not central in the project and therefore I have not included these actors in my stakeholder analysis.

To delve more into the interactions between the different actors within this network and how these influenced the eventual design of veiliginternetten.nl, I will first elaborate on each actor, its role and its stake in more depth.

4.2 Actors involved

This section describes the various actors that relate to the veiliginternetten.nl website. They encompass organisations, departments and companies that create, design, shape and regulate the website. Afterwards, I will give a small overview of other online means to shape the campaign as a whole, and how they are related to the website.

The Ministry of Safety and Justice

This ministry is the initiator and prime financier of the safe Internet use campaign. This ministry issued a budget to perform a two year campaign, during 2009 and 2010, aiming to prevent cybercrime. The ministry is responsible for upholding the law in The Netherlands, so the people can live together in freedom, despite their way of life or opinions[2]. Or simply put: "*to uphold justice and law in The Netherlands*" (Interview de Jong, campaign manager, 2011). Cybercrime was seen as a rising problem within the previous years, and the ministry is responsible to help the citizen prevent this crime or to fall victim to it. During 2008 research was done into the people's perception and awareness of Internet safety. Combined with the known statistics about cybercrime, they instructed the department Dienst Publiek en Communicatie to create a campaign which would raise awareness in the public about cybercrime. To stimulate the willingness to act, and to stimulate the acting towards a more safer Internet use. (Interview de Jong, campaign manager, 2011). More specifically towards the Safe Internet Use website, the goal was to "*provide quick and simple tools for people to guard themselves against cybercrime*" (Briefing Cybercrime, May 6, 2009).

Dienst Publiek en Communicatie (DPC)

Roughly translated as "Service Public and Communication", this department is part of the Ministry of General Affairs. DPC is the communication department for the government. Within DPC are campaign managers, who execute all campaigns issued by the various ministries. The Safe Internet Use campaign is one among many campaigns issued by the government, and is conducted, like all campaigns, under the brand name Postbus 51. DPC holds many specialists for the various fields that are needed to construct and successfully launch a campaign. Specialists on media, procurement (of TV and radio time-slots), internet, marketing and advertising. Due to the large history of organizing and executing campaigns, DPC has become a department of "*smart executives and advisers*" and practically acts as "*directors of the campaigns*" (Interview de Jong, campaign manager, 2011). Among these parties are research bureaus, online bureaus, marketing bureaus and advertising agencies.

Ministry of Economic Affairs, Agriculture and Innovation

This ministry, henceforth Economic Affairs, became involved midway the safe Internet use campaign. After the first year the main focus shifted from securing personal information to identity fraud and fraud with online transactions. This new focus aroused the interest of the Ministry of Economic Affairs in the safe Internet use campaign. Before the safe Internet campaign Economic Affairs already started a large awareness raising and stimulation project on internet: the project Digivaardig & Digibewust. This project aimed to educate the Dutch population as a whole in the use of computers and the internet. The execution of this project was given to ECP-EPN (slogan: platform for the information society). The website veiliginternetten.nl was included into this project Digivaardig & Digibewust. As both these ministries had their interest in a successful implementation of the campaign, the activities to steer the campaign had to be prevented of becoming ambiguous, let alone cause two different campaigns. For this, it was decided that the Ministry of Justice was to be leading. And of course was to uphold good interaction with it's fellow ministry to incorporate as many common goals as possible. But the message to Dienst Publiek en Communicatie was clear: The Ministry of Justice is the commissioning authority.

[2] Taken from the Ministry of Safety and Justice official website at http://www.rijksoverheid.nl/ministeries/venj

Research Bureaus

For the Safe Internet Use website, prior research was done by a bureau into the knowledge, attitude and behaviour towards the subject of cybercrime. The questionnaire was constructed by DPC, approved by the Ministry of Justice and the research was subsequently performed by a research bureau. DPC uses multiple research bureaus to do research prior to campaign, to test their products, and evaluate their campaigns.

Advertising Agencies

The results from preliminary research from the various bureaus were combined with the 'message' from the Ministry of Justice to be merged in a briefing, which was sent to an advertising agency. These went on to create the commercials, radio messages and website. Before launching these products, they were subjected to a test public. The aim of this phase was to see if a reflection of the target group understands the language used in the campaign. For the Safe Internet Use campaign it was concluded that it's message was clear, and that the (reflection of the) general public understood it's language.

Online Agencies

Rather then agencies that are found on the internet, online agencies refer to the various companies who programmed the veiliginternetten.nl website, or components of it. It started with the creative company Kong, who designed the outlook and concept of the website. This company in turn hired Refunk, to do the implementation of the website. Yet another party created a test which has been put on the veiliginternetten.nl website, for people to see how 'digi-aware' they are towards cybercrime. Apart from creating the website according to the goals as set out by the Ministry of Justice and DPC, they had to incorporate various requirements towards the accessibility (Webrichtlijnen[3]) and website standards (W3C[4]).

Users

The users of the website comprise of those Internet users that visit the website, read it's information and do or do not act out their tips. Users do not only visit the website by going to it's Internet location directly, they were also directed towards this website through the deployment of online actors as the Safe Internet Use campaign has an online component that goes well beyond the website. "*To make the website known, bureaus have been hired to buy entries in search engines, buy banners on various Internet pages and attract focus through various other online media and social networking sites.*" (Interview Krenn, online advisor, 2011).

[3] De Webrichtlijnen, for accessible websites with high standards, http://www.webrichtlijnen.nl/

[4] World Wide Web Consortium Web Standards, http://www.w3.org/standards/

Online actors and tools

Not only social actors became aligned to the safe Internet use campaign. Also online actors and tools were involved to “catch” the Internet user. I will distinction two types of online actors and tools that were aligned to the veiliginternetten.nl website. In the first type a popular specific website draws the attention of its users towards Internet safety. The second type are uses common online advertising tools to draw people's attention to the website.

The first type of online means to raise awareness, consists of the so called Stanislav viral. This viral takes over another website for a short while with a different message. DPC managed to align the popular Internet sites Habbo Hotel and the Marktplaats.nl home page to collaborate with this take over. The latter site is a popular Dutch website to buy and sell second hand products. Habbo Hotel is a meeting place for teenagers to interact socially. The Stanislav viral campaign consisted of a movie that would start when visiting your homepage on the Hyves Website. This social networking site would display a movie in which your personal information was incorporated into a movie depicting Eastern Europeans (supposedly with Stanislav as their boss) investigating your profile. Actual names and pictures, as well as the number of friends you had on Hyves, were used in the interactive movie clip.

Similarly, on the auctioneer website Marktplaats.nl (Market Place), upon selling or buying a product, a movie would appear (*over* your current web page) suggesting people are watching you. The two gentlemen in the movie acted as if they were detected, and quickly closed the movie. “*There was a link (redirection) made to the website, but many people didn't visit the veiliginternetten.nl website to get the message: Hey, I need to pay attention to what I do on Market Place*” (Interview Krenn, online advisor, 2011). These online activities were also created and launched by DPC, to achieve the goal to make people think about their online behaviour, on Internet spaces that were generally known or much used by the (Dutch) public and link it with the veiliginternetten.nl website.

The second type of online means that can be distinguished around the website is the tools employed to bring the website under the attention of the online public. To this end, banners were hired on other (again much used or known) websites, as well as keywords being entered into the largest search engine on the internet: Google. The banners comprise of small spaces on websites where an advertisement is shown of the Safe Internet Use campaign linking to the website. The search engine keywords consisted of entering keywords in the search engine application (AdWords) to have the veiliginternetten.nl website show up high in the ranks when searching for “veilig internetten”.

These combined efforts made the veiliginternetten.nl website have just over 400.000 visits during the first year, in which all online means were used. The second year of the campaign, which ran effectively for 5 weeks and excluded the Stanislav viral and Market Place take over, had just over 60.000 people visit the veiliginternetten.nl website (Intomart GfK Daphne 2010, Management Summary). The next section analyses how the interaction between the different actors relate to the design and intended use of veiliginternetten.nl.

4.3 A world of meanings

The variety of actors surrounding veiliginternetten.nl show various relations that have their effect on the website's eventual shape and use. Most notably, these are: the relation between the commissioner and executor, the different stakes the ministries have in veiliginternetten.nl's purpose, and how the website is used by DPC and ECP-EPN. I will refer to these relations as tensions. The notion of 'tension' could be perceived to be negative. However, I use 'tension' to indicate different views on the website, and different interests in it's shape and use.

The first tension exists between the Ministry of Justice and DPC. To inform the public on Internet safety, the Ministry of Justice envisioned a website that resembled a platform. Where people could look up not only simple tips to increase your online safety, but also information on how the ministry was working to prevent cybercrime, whom it collaborated with and to provide a vocabulary on Internet risks and dangers. A 'broad informative' point of view.
DPC however focused a lot more on the message that was to be sent to the public, and how to do this. A small and simple message that would 'stick' in people's minds. As experts in the field of communication, it was their job to narrow down the information to the most important message, and subsequently get this message effectively to the public. An 'effective communication' point of view. “*What concerns us in the campaign is just those tips on what to do. Done. The Ministry of Justice also wanted to display information on whom it collaborated with on the subject, and what else it was doing. All kinds of things that are not relevant for the goal of the campaign.*” (Interview de Jong, campaign manager, 2011)

The second tension arose between the Ministries of Justice and Economic Affairs. After the first year of the campaign, the topic switched from personal information on the Internet to your identifying information and transactions on the internet. The first topic comes mostly from crime and justice related problems, but have very little effect on the market or peoples ability to conduct transactions and trade. The second topic however, does involve matters in which the Ministry of Economic Affairs has a stake in. This is even bolstered by the project initiated this ministry: the Digivaardig & Digibewust project. In the middle of the campaign, Economic Affairs gained a stake in the success of veiliginternetten.nl, was subsequently added to the network, and contact between the different ministries and DPC was established. The tension thus arises whether the website is meant to prevent or lower cybercrime, or to stimulate the market and make online transactions more safe.

How the involves actors utilized the website for their own purposes and agenda, makes the third tension. For the Ministry of Justice and DPC the veiliginternetten.nl website was a means to make people aware of cybercrime. For ECP-EPN and the Digivaardig & Digibewust project, it was a means to make the public more “digi-aware” and “digi-literate” Internet users. A tension arises here between using veiliginternetten.nl as means to be safe online and as means to use computers and the Internet in a better way. Or more general formulated, DPC uses the website as means to further people's safety in society, whereas EPC-EPN uses the website as part to stimulate computer use. EPC-EPN were afraid that focussing too much on Internet risks might frighten potential users and hamper the stimulation of Internet use.

These tensions have their effects on the design of veiliginternetten.nl. The first tension results in the assessment of little or much information. Do we place all information on the website regarding whom the Ministry of Justice collaborates with? Is it supposed to become a platform (or library, repository, portal) or a small one-time message? The second tension results in weighing the emphasis on the different informative messages that are to be conveyed. Do we steer towards personal information or transactions? Do we encourage safe online payments or discourage unsafe online payments? The last tension results in the creation of a website to raise awareness and one that users visit to educate themselves on Internet safety. Do we design veiliginternetten.nl to educate the user on computer use or Internet use? To become more knowledgeable of the options and applications of computers and Internet or become more knowledgeable on the protective measures? Do we invite users to be aware of the risks or do we inhibit the use of malicious practices?

By having these ambiguous meanings of what the veiliginternetten.nl website ought to be, these tensions result in questions that affect the designing and eventual shape of veiliginternetten.nl. By adopting a science & technology studies point of view, the world of meanings surrounding the design of the website is (partly) revealed. How these tensions resulted in the material structure of veiliginternetten.nl is further elaborated on in chapter 6. But first I will provide insight into the future user that was envisaged by the network, and how this user was inscribed into veiliginternetten.nl.

5. The constructed user and real user of veiliginternetten.nl

Before I analyse the design and use of the veiliginternetten.nl website, I will first analyse the user that was constructed by the coordinating communication department DPC and taken into account when creating the website. Then I create a picture of the actual user. The chapter continues with comparing this constructed user with the actual user. The aim of this comparison is to discover possible misfits that might contribute to explaining a limited impact of user awareness raising technologies.

To make the comparison between the two types of users, I will use the overview of Punie (2000) as described in chapter 3. More specifically, in this chapter I will create a sketch of users based upon the three main components of ICT domestication that Punie discerns in his model Attitude, Knowledge & Capabilities, and Time-space. In this thesis I will refer to these three aspects as respectively attitude, knowledge and behaviour. By combining these aspects, a picture can be described about the user's stance towards Internet use, the user's knowledge of an Internet related vocabulary, and how the user integrated Internet use in his or her daily life. By applying this approach to both the constructed and real users, I can make them comparable.

Next to the model of Punie, I will use the taxonomy of user representation techniques by Akrich (1995) in the analysis of the constructed user. As there are several means to construct a user, the techniques described by Akrich provide the vocabulary to describe these means. The methods used by DPC to construct the envisioned user are related to the techniques as described by Akrich. This way I can analyse how the fictive user was constructed.

The empirical data used for this analysis is taken from research reports that were commissioned by DPC and executed by external research bureaus. DPC has commissioned external research bureaus to perform a survey on Internet users and their attitude towards Internet safety. The data used to determine the real user was obtained through qualitative interviews held with four Internet users. Using the three aspects of ICT use and the user representation techniques the analysis can be made of the combined data.

5.1 The constructed user of veiliginternetten.nl

The task of the DPC department was to create a campaign to reach those people who use the internet, and are prone to cybercrime. A person working in ICT security might be an Internet user in his or her daily life, but is not an Internet user that should be made aware of cybercrime. Likewise, a person who occasionally looks up information on the Internet but does not engage in online transactions nor has personal information on the Internet is not an Internet user prone to cybercrime. The constructed user of the veiliginternetten.nl website is thus one that uses Internet and is prone to cybercrime.

DPC used three out of the six techniques that Akrich has discerned to gain insight into the people's stance towards cybercrime. Market surveys have been used twice. Consumer testing has been used once. And to a less extent, the Other Products methodology was used. The two most relevant techniques are explicit representation techniques, implying that the users themselves are the sources of the user information (surveys and testing). The surveys consisted of one qualitative and one quantitative. The qualitative research involved interviews held with 19 people with different backgrounds, ages and occupations. The quantitative research involved 400 adults (18 years or older) and 200 youngsters (between the age of 13 and 18). Consumer testing was done just prior to releasing the created products. These were shown to a test audience after which their reactions were heard. Combined with the present knowledge of users from Internet applications, these combined techniques are used to analyse the constructed user of DPC.

Attitude

Through research conducted by DPC it was known prior to the campaign that many Internet users do not see cybercrime as an immediate threat. They think it won't happen to them. Similarly to being the victim of burglary or violence. "*If it's not close, it doesn't concern them.*" (Interview de Jong, campaign manager, 2011). A result from the Other Products technique. The first aspect of the constructed Internet users' attitude is thus one of passiveness towards cybercrime. This attitude is also the result of the qualitative research, concluding that the majority is aware of Internet risks, but does not pay much attention to it.

However, when explicitly asked during the qualitative interviews into people's attitude, a broader picture emerges. Nearly half of the public says to be worried about the risks and dangers of internet. Of these risks, most people are worried about computer viruses. Both as Internet risk in general as well as the risk that is most applicable to them. However, a majority (70%) feels they can protect themselves against Internet threats. This is bolstered by the fact that nearly all respondents of the research indicate themselves to be responsible for their Internet security. Other entities people deem responsible for Internet security are Internet providers and webmasters. For all these entities the youngsters deem them slightly less responsible. Also youngsters see themselves as the most responsible for Internet security, but also see their parents as having a responsibility.

An attitude that was assumed by DPC, but not directly affecting cybercrime was found within the youngsters: Those of the age 13-18 tend to overestimate themselves. Another aspect that can be attributed to the Other Products methodology. For DPC it was an attitude inherent to youngsters. "*They overestimate themselves. That also fits with that particular age and holds for more topics.*" (Interview de Jong, campaign manager, 2011). This characteristic of youngsters was taken into account when formulating the briefings.

Summarizing, the Internet users' attitude is primarily constructed by the measurement of vulnerability towards cybercrime; how worried users are and for what threats in particular; where users place the responsibility; and whether user can protect themselves. It was found that Internet users don't see themselves as possible victims, but do worry about viruses, and feel they should and can protect themselves. Youngsters however, overestimate the latter aspect. To construct the attitude of the user, qualitative and quantitative market surveys, as well as the Other Products methodology was used.

Knowledge

Knowledge on the subject of Internet risks deals both with knowledge *of*, and knowledge *how to*. Knowledge of the various risks of Internet use, of the various dangers, of the various effects of certain Internet use, etc. And knowledge how to use software, how to act safely, how to protect oneself. This knowledge can be obtained through education, but also through experience. The methods used to construct this aspect of the user is (just as attitude) largely based on the market surveys, but this time slightly expanded with consumer testing.

The knowledge of Internet risks and dangers is partially (but to great extent) constructed by measuring the familiarity of certain concepts and the vocabulary found in cybercrime. In one of the research projects, risks and dangers were conceptualized as Hacking, Grooming, Online bullying, Bot nets, Computer viruses, Phishing, Hoaxes, misuse of passwords, misuse of personal information, misuse of financial information and deception via online purchases. When asked about these concepts respondents were generally familiar with all of them, in very high percentages. Hoaxes were known to a lesser extend, and bot nets were rarely known by the respondents. The list of concepts was fairly extensive.

The knowledge of the concepts mentioned above were asked by posing the question whether one was familiar with the concept. This was not just done by posing the question *if* the person was familiar with the concept, but also *how*. The ways in which one could be familiar with concept was: the knowledge of the risk being out there, if one has fallen victim to it, or if one knew someone who experienced a situation with the risk. In other research the question was asked which risks and dangers were known, without providing concepts. Here the familiarity with hacking, SPAM, viruses, and child pornography were named. Towards the Internet as contact- and financial-economic medium, the risks of identity fraud, credit card fraud and deception with purchases were named. These risks and dangers could either be known to the user because they were applicable to the user, but could also be known because the users heard about them.

Another way of measuring people's knowledge and experience of Internet risks and dangers was by asking them the familiarity with protective measures. One of the results was s clear lack of knowledge of how can create secure communication. Nor do Internet users know how to check the security of their communication. It must be noted here that some respondents did know about the 'drie keer kloppen' (check three times) campaign issued by the government. This was a smaller campaign aimed at making safe online payments. But respondents subsequently did not have any experience with using the campaign information as they did not apply its recommendations. Another seemingly contradictory aspect of knowledge is found in passwords. Although nearly all respondents know that passwords should be hard to guess, only one respondent out of the 19 had knowledge and experience of actually constructing hard to guess passwords. There is a difference between knowing of, knowing how, to work with protective measures.

When the veiliginternetten.nl website and other means of the campaign were almost finished, they were subjected to a test audience to see if any of the terms used were known with the public. The test group that was used, was based on the target group for the campaign according to the campaign manager. My research however, did not include a broader analysis of this test group. Towards testing the website, "*The result from this test was that there were no unknown terms. A person might have made a remark, but there was no reason to change for example the word 'firewall'. People got it.*" (Interview de Jong, campaign manager, 2011). Consumer Testing added to the constructed user that an Internet user knows the jargon used in the website.

In summary, knowledge and experience of the Internet user encompasses the knowledge of a variety of concepts found in cybercrime. And to a lesser extent the knowledge of the means how one can protect oneself against these threats. Knowledge of Internet risks and dangers was based on knowledge in general, and experience with the risks, either by the person themselves or by knowing someone who had experience with the risk. After gaining insight on the user knowledge by conducting survey research, DPC subsequently tested their ideas on a test audience, that was knowledgeable on the terms used. This knowledge aspect of the constructed user thus was primarily obtained through techniques of market surveys and consumer testing.

Behaviour

The third component of Punie's model that I use to analyse the construction of the user is "time-space" . As this notion is a somewhat abstract, I will refer to it as one's behaviour towards ICTs. When do you use it? How often do you use it? What place has it been given in the household? Or: What place has it been given in one's Internet use? With these questions a picture is formed how one's behaviour is towards Internet and it's risks and dangers. This part of the construction of the user was also largely constructed using market surveys, with a small notion of the Other Products methodology.

Behaviour is roughly divided into two categories: One's behaviour towards Internet use, and the behaviour towards the risks and dangers. Both market surveys create a picture of the Internet use of their respondents. By asking how many hours a day one uses the internet. Whether one uses the Internet on a daily basis. And if one could live without the internet. Apart from these questions that mainly do with the 'time' aspect of Internet use, questions were asked what the Internet was used for. What 'space' it was given.

An important difference in behaviour was found between youngsters and adults. Among all the activities that are done on the Internet youngsters use the Internet more for communication and entertainment, whereas adults use the Internet more for transactions. "*The younger target group, of that we know they occupy their time more with communication and the adults use it more for transactions.*" (Interview Krenn, online advisor, 2011). Both these groups also use Internet to look up information. These activities combined make up for the behaviour towards internet. This knowledge about the user is where the Other Products technique was used to complement the construction of the user, resulting in two types of behaviour. One for youngsters and one for adults.

The other aspect of behaviour is that towards safe Internet use. What one does to prevent cybercrime. The first set of actions performed is of a technical nature: If the respondents use virus scanners, SPAM filters and firewalls. The second set concerns codes of conduct: For using their online personal information, for buying and selling products online, and engage in, and maintain online contacts. Breaking down behaviour towards safe Internet use even further, respondents were asked to what extent they apply safety measures when using the internet. If one manually runs a scan with their anti-virus software. If one pays attention to secure communication marked by the 's' behind the 'http' in the web address. If one thinks about risky behaviour when engaged in online transactions or downloading. Together, these questions construct the behaviour of Internet users towards safe Internet use.

With the market surveys done by DPC, combined with the knowledge already available, the behaviour of Internet users gives a comprehensive picture. It's measured through Internet use, time spend on the internet, and subsequently on the use of protective measures and how these are applied. The constructed Internet user uses the Internet daily, for a multitude of purposes. But the time spend on safety measures and the diversity of them is limited. With this last aspect of users analysed, the complete constructed user can be described.

The constructed user of veiliginternetten.nl

In this section I will reconstruct the Internet user that was in DPC's mind when designing the veiliginternetten.nl website, the constructed user, by combining the above mentioned factors of attitude, knowledge and behaviour. The Internet user prone to cybercrime is one that *thinks* he or she is not prone to cybercrime. Who is knowledgeable on the various risks, but thinks he or she will not fall victim to it. Who is an Internet user who thinks that the responsibility lies mainly with themselves and think they can protect themselves. In the case of youngsters however, these Internet users overestimate themselves.

Although the constructed user knows many risks and concepts, they have little experience with them, similarly for protective measures. They are known, but how to utilize them properly is generally not known. This is bolstered by the behaviour of the envisaged user. The Internet is used on a daily basis and for many purposes. But for many of these purposes protective measures are not taken, or not taken properly.

5.2 The real user

This section describes the real user by analysing the data from the first round of interviews with four Internet users. It should be noted here that the government campaign has run it's course, and the attentive reader could ironically point out that the real user is of course different from the projected user. They have been made aware by the campaign! However, none of the respondents was familiar with the website, and when asked about the commercials on radio and TV, none could recall ever to have seen it. This is mostly due to the respondents dislike for commercials in general, or low use of the media in general. That being said, the subsections from the interviews included the three aspects from ICT users as used from the model from Punie.

Attitude

To establish insight into the attitude of the real users, questions were asked if the respondent felt safe while using the Internet and if they felt they were acting in a safe manner. If they had a general (dis)trust in the internet, and whether they trusted certain website more then others. More specifically, they were asked about their attitude towards online transactions and personal information on the internet.

There is a general consensus among the respondents that the Internet is a trustworthy medium. None of the respondents had a general distrust for the medium even when keeping the risks and dangers in mind. They perceive it as a very useful technology and don't associate it any more or less with risks and dangers then other aspects of daily life. As Ilona points out: "*If people are out for your information they will find that anyway, with or without internet.*" This attitude was found in all respondents, who gave similar examples how risks and dangers are aspects of daily life, and not to Internet in particular. None of them see a reason why they should fall prone to cybercrime.

Furthermore, all four respondents see safe Internet use primarily as their own responsibility. None of them assume the government, Internet providers or webmasters to further this cause. In two cases however, "the husband" and "a friend that knows a lot about computers" were referred to as the security experts when asked what would happen if something went wrong. In these cases, the responsibility towards a protected computer was delegated to trusted relatives. But generally the respondents perceive their safety online as a matter of common sense. The same common sense they apply to activities outside of computer- and Internet use.

Towards one's own responsibility on the internet, the respondents feel they're acting safely. That they apply their common sense to the various ways in which they use internet. But there are slight discrepancies here. Wil, the 79 year old lady, acknowledges herself to be little knowledgeable of Internet banking. And subsequently doesn't engage in the possibilities of online banking. On the question if she tries to prevent problems on the Internet she answers that "*one shouldn't make use of risky technologies one doesn't understand*". Whereas the other, more 'internet savvy' respondents referred to certain acts like paying attention to the e-mails you receive. None of the respondents acted in a very light hearted or unsafe manner.

The attitudes shown towards Internet use and it's risks and dangers is of a positive nature. Internet is a useful technology to which the respondents didn't express concerns about it's risks. And the risks that they knew were part of Internet use were no more or less applicable to them then other risks in daily life. The respondents felt the responsibility lies with them, and they act so accordingly.

Knowledge

Knowledge of and experience with the various Internet risks and dangers was established by asking two different types of questions, with resemblance to the research done for the projected user. Namely if the users were knowledgeable about Internet risks and dangers, and how experienced they were with these. First the question was asked if they could name risks and dangers, and then if certain ones were familiar to them. Then it was asked what their experience with these risks were. Next to this, it was asked if they've seen or read articles about cybercrime in the media, and if they've seen any user awareness campaigns.

When asking the respondents to name Internet risks the most prominent one was computer viruses. For the elderly woman, this was the only risk for Internet use. The other respondents named hacking, suspicious e-mails and identity fraud. Jan could name the most, as it was his duty to be knowledgeable on the subject. He even named the dangers of having mobile phones connected to the internet, and was the only one to point out that one must be wary when opening attachments or suspicious files. Ilona showed yet another distinctive piece of knowledge on the subject: Although she never heard of phishing, she was the only one who named skimming, a form of credit card fraud.

When faced with other forms of Internet risks, the general answer was one of ignorance. Hoaxes, bot nets and grooming were not known by any of the respondents. However, when Ilona was asked about her son, she did mention that she was very cautious with chatrooms. And that she was worried when her son would be engaging with this. When asked if she was worried for grooming she couldn't tell. Grooming is the practice of 'chatting up' youngsters, by adults with ill intents, via chatrooms. The mother was certainly aware that this was a risk associated with Internet use, but didn't know the term for it.

The respondents were more knowledgeable about protective measures then they were with the risks. When asked about the knowledge of safe Internet use, all but the elderly woman could name plenty. "*Careful with e-mails, blocking your profiles on social networking sites, log out after you used Internet banking, perform online payments via iDeal* (a service created by Dutch banks for Internet payments)". The means to protect oneself are rapidly named by Marije, the 37 year old optician. For every form of Internet use she could name an accompanying act to make it a more safe one. The CEO of a small company, Jan, could name plenty as well and even referred to a 'kwaliteits-zorg-systeem', a code of conduct the employees of his company were to adhere to when using the internet.

Knowledge of cybercrime and it's related issues was quite substantial with the real user. Apart from specific risks all respondents provided reasonable knowledge on both the risks as well as protective measures. Also the familiarity with the dangers of Internet and the protective measures was present in decent extent. The real user is quite knowledgeable on the subject of cybercrime.

Behaviour

To gain insight into the behaviour towards and on the Internet questions were asked like: How much do you use internet? Are you on the Internet a lot? What is it you do on the internet? Could you live without the internet? And: Do you have personal information on the internet? Towards Internet safety, questions were asked if the respondents used certain software to protect themselves, if they did (or didn't) particular acts to further their safety, if they tried to prevent risky situations, and how they handled their personal information on the internet.

During all interviews it became quickly apparent that Internet use is a daily practice. From the day-to-day activities of Internet in private life and for work related purposes to checking the e-mail on a daily basis. For two respondents daily life could not be imagined without internet. Not only the elderly woman, but also the thirtysomething woman could very well imagine life without it. "*When I take a two week holiday I can easily live without the Internet as well*".

Internet was used for about all activities one can come up with: e-mail, searching for information, online purchases, social networking, online communication. From buying a painting to using Skype with a relative in Canada to requesting invoices; the Internet is used for a whole variety of different means.

But, although the respondents were engaged with all these activities, their enthusiasm for security was not so great. Yes they had a firewall, and a relative installed some anti-virus software, but how these worked and what the specifics of any of these products were was not found in the behaviour of the respondents. Manual scans for viruses were not performed by the respondents, and updates for protective software were just 'accepted' and quickly clicked away whenever it popped up on their screens. The most striking example was found in passwords. Although three of the respondents knew that a decent password was to provide a high level of security, they were reluctant towards actually behaving accordingly.

The use of Internet and its protective measures is for the respondents a daily routine. Using Internet daily for a variety of purposes, but showing little behaviour towards safe Internet use. Apart from the CEO who was partly talking on behalf of his company. Real users spent little to no time on protective measures, let alone that it was part of their behaviour to act accordingly. An interesting exception to this is the elderly woman who, by not using Internet for transactions and not putting any personal information on the internet, was behaving the safest. Now that I have described the last aspects of the real user, I can create a total picture of the real user and subsequently compare this to the constructed user.

The real Internet user

The analysis of the Internet user who will be using the veiliginternetten.nl website was done with the interviews held with four individuals who all use Internet on a daily basis. One uses Internet more then the other, but all have activities that are done as a daily routine. "*Checking e-mail every evening*". For two of them the Internet is by now a necessary part of life. And the Internet is used for a great variety of practices.

Internet is used with no more or less caution then with other practices in daily life. That it is one's own duty to act responsibly with the Internet is a shared opinion of the respondents. And towards this technology, the real user thinks he or she has sufficient knowledge to do so. However, this knowledge has not yet concretely found it's way to practices. The reluctance to see themselves as the target of criminal activity seems the primary cause of this. The real users are aware that cybercrime is real, and have read or heard the occasional article in the media. But they see no reason why they should be more cautious to Internet in particular. Marije: "*I don't constantly think about my house being broken into either*".

The real user has given some thought to their Internet use and are aware of most common aspects of safe Internet use. And if a computer has caught a virus, the real user refers to their spouse or relative that will fix the problem. For certain criminal practices that the respondents also know it's existence, just not the word, they have a good set of practices to prevent most harm. With this picture, I will now compare them with the constructed user.

5.3 Comparing the constructed user and the real user

By using qualitative interviews for representing the real user, a rich picture of Internet use is revealed. The constructed user was analysed by using the market survey research that was commissioned by the coordinating department DPC. The comparison between the constructed and the real user takes an in-depth look into the user and reveals insights that could contribute to develop more effective user awareness tools for stimulating safe Internet use. The outcome of my analysis of the real user does overlap with the broad research performed prior to the campaign. To a certain extent it can be argued that the results of my interviews held with real Internet users is a small subset of the qualitative research issued by DPC. However there are slight discrepancies between the individual Internet users and the generalized Internet user constructed by DPC. Using semi-structured interviews, qualitative interviewing does give a richer picture into the real user.

Concerning the Internet user's attitude towards safe Internet use, when generally asked if Internet users see themselves as possible victims of cybercrime the constructed user is one that does not see him- or herself as such. But the real user is aware that cybercrime could affect them. They knowingly don't give it much attention as there are so many things in life to look out for. It's not the case that Internet users don't know. It's rather that they don't care. They are aware, but not willing to put that into practices when using the Internet or give it's safety much attention. This is also seen in their time spent on safety measures, but there is another thing about the real user's attitude.

Real users care about more then just their own safety on the internet. In the interviews used for the constructed user however, no such question was asked. But when asked during the question about the known risks and dangers, Ilona pointed out that she knew very little about children and the internet. Something she definitely wanted to change before her son would engage with the wide variety of Internet uses. Also Wil mentioned the use of Internet by her granddaughter. (And how this four-year-old knew more about it about her!). "*users aged 13 and over act independently on the Internet without adult supervision*" (Intomart GfK Daphne 2010, Management Summary) was given as reason why the campaign was concerned with that particular age group. However, people could be looking for risks and information that affect their (grand) children's use of Internet as well.

Being knowledgeable on risks and dangers of Internet was very similar between the constructed and real user. In both cases the respondents knew many terms like viruses, spam, and information theft. Similarly for protective measures, both the constructed user and real user can name a variety of practices that reduce the risks and dangers associated with Internet use. Or when asked for specifics, many terms were familiar to all of them. Towards knowledge, the constructed user and real user show great resemblance. But there is a difference between what they know, and why.

The interviews with the real users show that more protective measures are known with the Internet user. When using a different computer then your own, logging off after Internet banking or other websites that requires a user to log in, is such an example. But the real user shows another distinctive approach to their knowledge of safe Internet use. It is accustomed to their particular Internet use. Jan, as employer and owner of a company, knows many protective measures concerning the safety of the company's computer network. Ilona, who keeps an eye at Internet use by her child, knows how to secure her online personal information on Social Networking Sites, and Marije, who uses Internet for many personal activities, knows what's important when making online purchases. Wil, the elderly lady even shows an unusual piece of safety awareness, namely that when faced with a complicated technology (the Internet itself), she doesn't partake in many of the purposes and thereby prevent risky situations to even occur. The knowledge of cybercrime and it's related aspects of safety are generally the same between the constructed and real user, but the real user shows this knowledge to be mostly relevant to *their* Internet use only.

What both the constructed user and real user show in the aspect of behaviour (time spend on, and on what activities) towards Internet use, is a daily use and a variety of purposes. But time spend on protective measures is in both cases very little compared to their knowledge of these measures. The constructed answers the 'what' question, but only little the 'why' question. What protective measures are available, but not why users do or don't use the measure. Ilona knows about firewalls, anti-virus software and automatic updates, but has fully delegated the responsibility to have this software up and running to her husband. Similarly with Marije, her susceptibility to viruses (her greatest threat to computer use even) is not completely converted to practices because she has a friend that can repair the infected computer. And with all users, it is known that difficult passwords, multiple passwords and changing passwords are a useful protective measure. Yet none of them has 'hard' passwords, nor changes them regularly, nor has a whole variety of them. Jan is very aware of this, but can't find an easy practice yet to act accordingly. "*I read some about passwords, and using sentences can make you remember longer, therefore harder to guess passwords. But incorporating all measures would be more of a problem then the risks of having only a few, easy to remember passwords.*"

There is another broader picture emerging in the real user and their behaviour towards safe Internet use. This is the picture of Internet use in general. When it is used, and for what purposes. The constructed user uses Internet a number of hours on a daily basis, and for a wide array of purposes. But the real user shows quite some diversity in this description. The entrepreneur uses Internet the most of all respondents, but does this nearly completely during working hours, for purposes of work, in an ICT environment that is maintained by an ICT specialist. And uses Internet very little at home and barely for private purposes. For Ilona however, this is the opposite. She barely uses Internet at work, but does so to a great extent at home, for private use. Using Social Networking Sites, shopping, looking up information, booking vacations. Many purposes that involve private and personal information, and transactions. In the case of the elderly woman, she does use Internet on a daily basis, but does not use Internet for many purposes. Mainly checking e-mail, looking up information on her son's racing team and the occasional communication with her relative in Canada. This makes the Internet use of these three users conform to 'daily use' as well as 'different purposes'. Yet the circumstances under which this Internet use takes place differs greatly. And although the practices of looking up information and using e-mail dominate the category of Internet usage, there is no fixed set of practices that applies to all Internet users.

By using semi-standardized qualitative interviews, I created a broad picture of Internet use in the real user. Through analysis of the constructed and real user there are discrepancies found that indicate a broad variety of users (I used only four) and uses. But it is also not surprising that the real user greatly resembles the constructed user. The average Internet user does indeed not know all the protective measures, and certainly did not include them in the daily practices. Internet users like the technology, use the technology, and show a healthy amount of common sense and scepticism towards it's use. They are not specialists in the field, but also cannot be expected to be. Even when considering that the digital literacy of the public has increased over the recent years, the constructed user still resembles to a great extent the real users' attitude, knowledge and daily practices. But there is more to it.

An 'Internet user' is not just defined by daily use and a variety of practices. The circumstances under which people use Internet differ (company network vs. home computer), as does the set of purposes the Internet is used for. And Internet users are not completely unaware of the risks and dangers. They do know, but don't care too much as the risks and dangers of Internet do not pose a significant threat to daily life as compared to physical well being and general theft and abuse. However, my small empirical research among the real Internet users also finds that the gap between awareness & knowledge and acting still is large. Actually only one of the four respondents acted according to her (lack of) knowledge by actively choosing for non-use. For the other three respondents, non-use was no option.

With this picture of Internet users in mind, the next chapter analyses how the constructed user was inscribed into the website's script and how this script was de-scribed by real users.

6. The script of veiliginternetten.nl and it's de-inscription

The website of the Safe Internet Use campaign was made to reduce cybercrime and stimulate safe Internet use. (Interview de Jong, campaign manager, 2011). The website had to contain certain information and was to be used for a specific purpose. (Briefings 2009 and 2010). Furthermore, it was to be used in a certain way, and to counteract certain other actions. This chapter builds on the concepts of script, inscription and de-inscription to analyse how these goals were inscribed into the website, resulting in the script of veiliginternetten.nl. A script that can have an inviting and inhibiting effect on it's users' (safe) use of internet. And subsequently, how this script was de-scribed by the actual user. The analysis consists of the inscription of the goals and constructed user into the website as done by DPC (I will use Jelsma's notion of design logic), a script analysis of the website itself, and an analysis of how the real user has used the website (user logic).

6.1 The design logic of veiliginternetten.nl

To start the script analysis I will look how the designers incorporated the constructed user and their vision of the world into the website. What users were assumed to know and do, and how the goal to stimulate safe Internet use was put into the various components of the website. This is done analysing the briefings that were made by DPC and were for describing the commission assignment for the web designers. The first briefing is from 2009 and outlines how the website was to be constructed. The second briefing was made in the middle of the campaign and outlines how to continue the campaign with a different goal. Although one briefing concerns the campaign as a whole, and the other specifically towards the website, the briefings give a decent amount of data to analyse how the website ought to be used.

In the first briefing an outline for a script was provided how users have to look up information. In four steps the users would find tips regarding their Internet threat, it's symptoms when being a victim, how it relates to Internet use, and which form of cybercrime was present in that topic. The briefing outlines how a user should be informed on these four aspects of a topic after either searching for it, or when using one of the options from the menu. Different points of entry into the topic were deemed possible, and should all invite the user to be informed on the four aspects. Making the first aspect of inscription one of a curious user that would specifically be provided various aspects of the users' topic of interest.

Although safe Internet use encompasses the awareness that one could be a victim of cybercrime, this was not seen in the first briefing as to be inscribed into the website. It was not seen as part of the website to let users know they could fall prone to Internet threats. They could look up symptoms, but not made aware that they could already have been a victim. The second briefing however incorporated this element as one of the "*attitude-objectives*" (Intomart GfK Daphne 2010, Management Summary) aiming to enhance the users realization that they could a potential victim of Internet crime. Inscribing that users should be made aware was to be done when the topic changed from online personal information to online transactions. As in the subsequent paragraph the latter website is analysed, veiliginternetten.nl was inscribed with the goal to make users aware that they could be a victim.

What also changed during the campaign, was the emphasis on who was responsible for one's safe Internet use. The projected user prior to the campaign was one that placed the responsibility of safe Internet use to be with themselves. In the first briefing however, the website was "*to convey that the government was providing help and comfort*" (Briefing Cybercrime, May 6, 2009). In the second briefing, the constructed user was one that did not realize they could become the victim of cybercrime, similar to the prior situation. Only halfway into the campaign this was subsequently seen as "*communicative challenge*" (Intomart GfK Daphne 2010, Management Summary) as the campaign had to make people aware of the potential dangers of internet, without discouraging them to use this technology. Only during the second half of the campaign, the website was to induce the responsibility for safe Internet use into the behaviour of the user.

Up till this point there are similarities between the constructed user and how this user was inscribed into veiliginternetten.nl. A user that is not fully informed, could use tips, and be made aware that they too can be a victim, and should bare responsibility. What was however not inscribed, was the variety of users. A generalized user was used in both the first and second briefing. Veiliginternetten.nl should be a "*site for the public, accessible to all*" (Briefing Cybercrime, May 6, 2009), and later on, "*induce the same results to both youngsters and adults*" (Intomart GfK Daphne 2010, Management Summary). The knowledge different users have of Internet use was inscribed using only a generalized user.

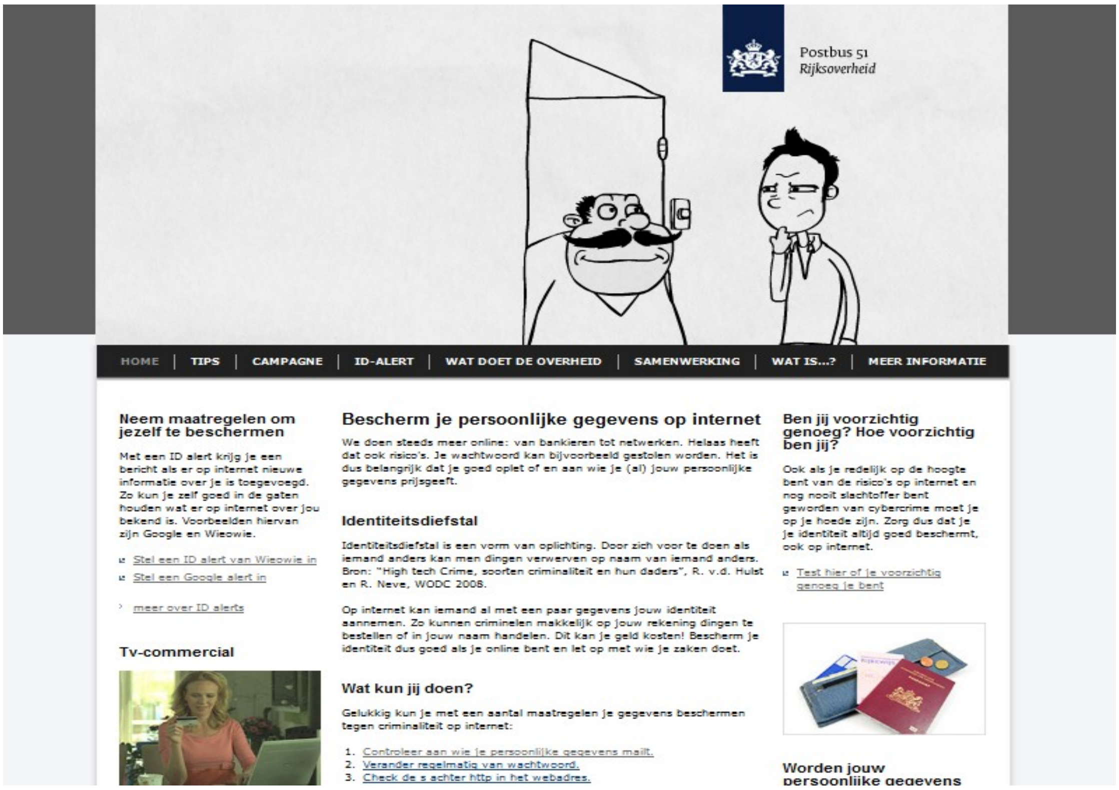
Inscribing 'cybercrime' seemed to be a large aspect. Cybercrime was not simply demarcated to online personal information and online transactions, cybercrime was inscribed in a much broader way. During the first briefing veiliginternetten.nl was to go "*a step beyond the campaign*" (Briefing Cybercrime, May 6, 2009) and should include many forms of cybercrime, also those which were not used in other aspects of the campaign. This broad inscription was also seen in the subsequent year, where cybercrime was to be expanded with "*misuse of technical shortcomings in the security of internet*" (Intomart GfK Daphne 2010, Management Summary).

Another aspect of cybercrime was also inscribed into the website. Namely that the different forms of cybercrime change over time and importance. The first briefing deemed it not only "*of importance*" (Briefing Cybercrime, May 6, 2009) that the information should be actual (recent), it was even called "*essential*" (Briefing Cybercrime, May 6, 2009) to keep it updated. Inscribing this into veiliginternetten.nl found it's way into the second briefing pointing out that another communicative challenge is: "*to protect oneself means taking different measures that occasionally change due to the nature of cybercrime*" (Intomart GfK Daphne 2010, Management Summary). Cybercrime was inscribed very broadly, and as changing over time.

Using just two briefings, various aspects of the user, cybercrime and the campaign's goal were found. How veiliginternetten.nl was to change the Internet user's behaviour, was by inscribing a generalized user that had to be made aware of Internet threats that could affect him or her. This generalized user too had to take measures to stimulate inter safety. To realize this, the users had to be provided with a searchable source of information outlining tips, symptoms and a broad range of the different forms of cybercrime. However, in the first briefing also quite some attention was given to the requirement to inform the user about the governmental actions to stimulate Internet safety. Clearly, the design context had not one consistent design logic from which the design specification were formulated. There were multiple interests at stake.

6.2 The script of veiliginternetten.nl

This section describes the script of veiliginternetten.nl. What can users do when they visit the website? What enables the website the users to do? In analysing the website, I assumed that Dutch viewers will approach websites by looking from left to right, and to read from top to bottom. The analysis comprises of the options that are available on the website, and what can be done on the various pages that the website consists of. Next to this, at looks at the ways in which awareness can be stimulated, and what tips and tools are provided. To make this analysis, I started by dividing the homepage into sections (see fig. 3 & 4). From here, I analysed how the website can be used to stimulate safe Internet use.


Postbus 51
Rijksoverheid
HOME | TIPS | CAMPAGNE | ID-ALERT | WAT DOET DE OVERHEID | SAMENWERKING | WAT IS...? | MEER INFORMATIE

Neem maatregelen om jezelf te beschermen

Met een ID alert krijg je een bericht als er op internet nieuwe informatie over je is toegevoegd. Zo kun je zelf goed in de gaten houden wat er op internet over jou bekend is. Voorbeelden hiervan zijn Google en Wieowie.

- Stel een ID alert van Wieowie in
- Stel een Google alert in

› meer over ID alerts

Tv-commercial

Bescherm je persoonlijke gegevens op internet

We doen steeds meer online: van bankieren tot netwerken. Helaas heeft dat ook risico's. Je wachtwoord kan bijvoorbeeld gestolen worden. Het is dus belangrijk dat je goed oplet of en aan wie je (al) jouw persoonlijke gegevens prijsgeeft.

Identiteitsdiefstal

Identiteitsdiefstal is een vorm van oplichting. Door zich voor te doen als iemand anders kan men dingen verwerven op naam van iemand anders. Bron: "High tech Crime, soorten criminaliteit en hun daders", R. v.d. Hulst en R. Neve, WODC 2008.

Op internet kan iemand al met een paar gegevens jouw identiteit aannemen. Zo kunnen criminelen makkelijk op jouw rekening dingen te bestellen of in jouw naam handelen. Dit kan je geld kosten! Bescherm je identiteit dus goed als je online bent en let op met wie je zaken doet.

Wat kun jij doen?

Gelukkig kun je met een aantal maatregelen je gegevens beschermen tegen criminaliteit op internet:

1. Controleer aan wie je persoonlijke gegevens mailt.
2. Verander regelmatig van wachtwoord.
3. Check de s achter http in het webadres.

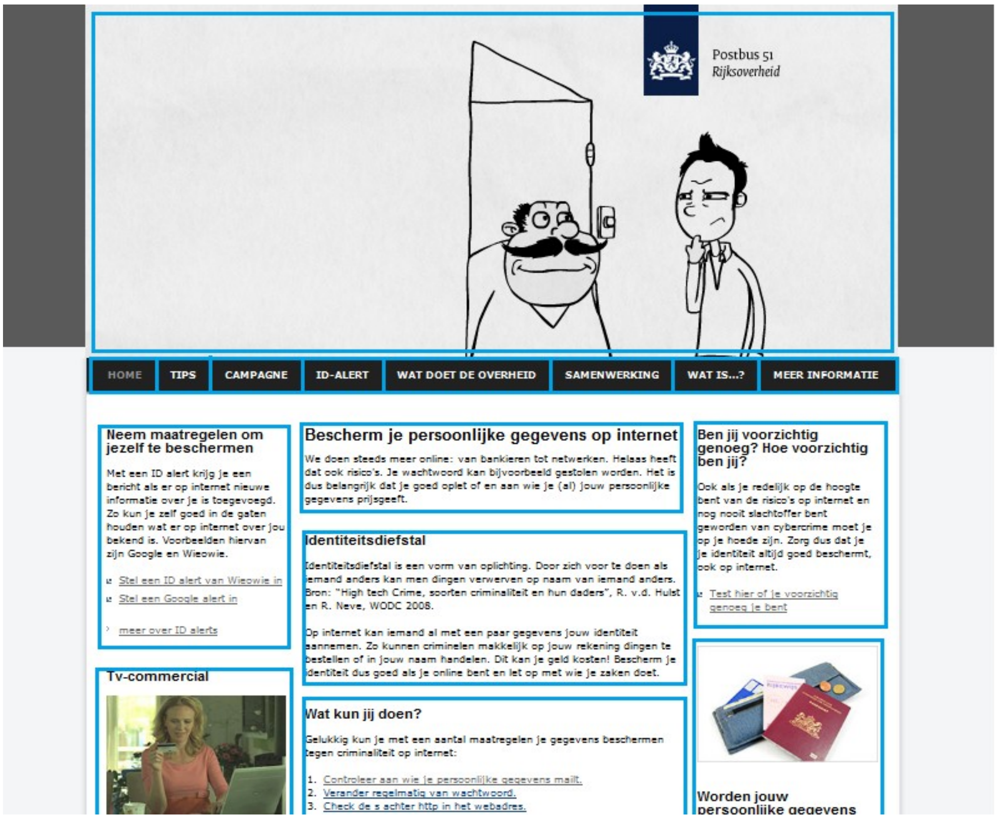
Ben jij voorzichtig genoeg? Hoe voorzichtig ben jij?

Ook als je redelijk op de hoogte bent van de risico's op internet en nog nooit slachtoffer bent geworden van cybercrime moet je op je hoede zijn. Zorg dus dat je je identiteit altijd goed beschermt, ook op internet.

- Test hier of je voorzichtig genoeg je bent

Worden jouw persoonlijke gegevens

Fig. 3: The veiliginternetten.nl website.



Neem maatregelen om jezelf te beschermen

Met een ID alert krijg je een bericht als er op internet nieuwe informatie over je is toegevoegd. Zo kun je zelf goed in de gaten houden wat er op internet over jou bekend is. Voorbeelden hiervan zijn Google en Wieowie.

- Stel een ID alert van Wieowie in
- Stel een Google alert in

› meer over ID alerts

Tv-commercial

Bescherm je persoonlijke gegevens op internet

We doen steeds meer online: van bankieren tot netwerken. Helaas heeft dat ook risico's. Je wachtwoord kan bijvoorbeeld gestolen worden. Het is dus belangrijk dat je goed oplet of en aan wie je (al) jouw persoonlijke gegevens prijsgeeft.

Identiteitsdiefstal

Identiteitsdiefstal is een vorm van oplichting. Door zich voor te doen als iemand anders kan men dingen verwerven op naam van iemand anders. Bron: "High tech Crime, soorten criminaliteit en hun daders", R. v.d. Hulst en R. Neve, WODC 2008.

Op internet kan iemand al met een paar gegevens jouw identiteit aannemen. Zo kunnen criminelen makkelijk op jouw rekening dingen te bestellen of in jouw naam handelen. Dit kan je geld kosten! Bescherm je identiteit dus goed als je online bent en let op met wie je zaken doet.

Wat kun jij doen?

Gelukkig kun je met een aantal maatregelen je gegevens beschermen tegen criminaliteit op internet:

1. Controleer aan wie je persoonlijke gegevens mailt.
2. Verander regelmatig van wachtwoord.
3. Check de s achter http in het webadres.

Ben jij voorzichtig genoeg? Hoe voorzichtig ben jij?

Ook als je redelijk op de hoogte bent van de risico's op internet en nog nooit slachtoffer bent geworden van cybercrime moet je op je hoede zijn. Zorg dus dat je je identiteit altijd goed beschermt, ook op internet.

- Test hier of je voorzichtig genoeg je bent

Worden jouw persoonlijke gegevens

Animations

Menu

Various content briefly presented

Fig. 4: The veiliginternetten.nl website broken down into the different uses.

The first thing a user of the website will notice is the showing of an animation. The first effect of use is to invite the user to watch three short clips that contain tips that stimulate safe Internet use. The animation clips are without sound. They consist of a protagonist who portraits situations in daily life that are analogous to Internet behaviour. Simplistic as the animation clips are, they are self explanatory and easy to understand. These animations are at the top, and are the first to be viewed.

In the first clip, the protagonist rings a doorbell after which a man opens. The protagonist examines the man by yanking his moustache and taking a closer look at the man with the use of a magnifying glass. A text then appears in the clip: Tip 1: Check who you mail your personal information.
This video fades into an animation with the second tip (Regularly change your password) and similarly for the third (Check the 's' behind 'http'). These three clips are continuously played unless the user decides to stop it using the 'pause' button in the upper right corner, indicated by two vertical lines.

From here, the user is invited to either a selection from a menu, or read a small introduction to the various content and options. The menu (as indicated in fig.4) is a rectangular black box with 8 white words or texts, demarcated by white vertical lines. With these 8 buttons, the various content of the website is accessible. From left to right, these read: Home, Tips, Campaign, ID-Alert, What the government does, Cooperation, What is...? and More information. 'Home' is in grey, indicating that this is the section where the user is currently.. At this point, the user is invited to make a selection from the available options. However, the user is also inhibited to search for specific information, as a search option is lacking.

If the user does not choose an option from the menu, a user can continue to read the information presented on the rest of the website. Here the script becomes very ambiguous: Divided into three columns, actions that can be performed are: reading information, watch the TV commercial, read who collaborated with the government on the project, do a test to see how careful you are on internet, report abuse of your online information, use tools to alert you when (your) personal information becomes available on the internet, and see 'what you can do': tips that stimulate safe Internet use. Both the menu and the provided options invite the user to choose that part of safe Internet use that the user deems important or otherwise appealing.

Apart from two sections, veiliginternetten.nl's script after choosing a section turns into a 'read me'. After nearly all options, the user is presented with a long text, containing numerous hyperlinks to other Internet locations. The websites script then turns into a text, that expects the user to invest time into the website, and inhibits the user from continuing with the website: The user is invited to leave the website and continue on a different website or part of the internet. An example is the test, where the user is redirected to a test on a different website. After making the test (and reading a good deal), the user is more or less inhibited to returning to the website, as the test site offers no return option.

The two sections that do not invite the user to a large piece of text are 'campaign' and 'ID-Alert'. 'Campaign' will redirect the user to a short film that they can start and view at their own discretion. After this film however, the user is not presented with options to continue reading or working on that particular Internet threat (identity theft). Choosing 'ID-Alert' will redirect the user to a short description of what the ID-Alert is, and then invites the user to visit an Internet location where the ID-Alert can be activated. On the homepage, two options are presented that redirect the user away from the website.

Veiliginternetten.nl has a script that includes both user awareness as well as tips and tools do to so. These two aspects of Internet safety are, in my view, the ways in which safe Internet use is stimulated. Examples found of user awareness are on the front page (“Protect your personal information on the internet.” and “Are you careful enough?”). Veiliginternetten.nl mentions on several places that one must act safe online, be cautious, and the website informs the user that this responsibility is on behalf of the user now. But by placing a section on the website entitled “What the government does” the website doesn't completely delegate this responsibility to the user.

Similarly, tips and tools are presented on various places on the website. One can read tips ("Check who you mail your personal information", "Check the 's' behind 'http'", and "Change your password regularly") and find tools (The ID-Alert, safety test and reference to anti-spyware). In providing the Internet user with tips and tools, the script of veiliginternetten.nl invites the user to adopt a number of tips and use tools. But also these tips and tools have an inhibiting character, and redirect the user away on many places in the text outlining the information.

The script logic of veiliginternetten.nl is then to watch short animations, make a selection from the presented menu or its elaborated sections below, and invest time in reading the presented information. Exceptions to this are the viewing of a short film, or to engage in an online test. The last use of veiliginternetten.nl is to either exit the website, or follow one of it's hyperlinks to an external location.

This latter notion, users being directed away from the website, is why Verbeek's (2005) concepts of invitation and inhibition are useful in describing the script of veiliginternetten.nl. There are many 'paths' a user is invited to follow, but many of those redirect the user away from veiliginternetten.nl. Without providing the option for the user to go back to the website or look up a different aspect of Internet safety. By having users provide so many invitations to continue reading or working with an aspect of Internet safety away from veiliginternetten.nl itself, the website as a whole is inhibiting the user to engage with the veiliginternetten.nl website itself.

With this script in mind, the following section analyse how veiliginternetten.nl was subsequently perceived by the user, who de-inscribe the website according to their own user logic.

6.3 The user logic of veiliginternetten.nl

After the respondents were given a week to use the website, they were interviewed in a second round of interviews. Central to these interviews were four topics: Their general impression of the website and what they did with it; the knowledge and awareness of Internet risks; their Internet behaviour; and acts and tools to stimulate safe Internet use. Three users had taken notes, and took a piece of paper with them to aid them in the interview.

The first question was deliberately an open one: What is your general impression of the website? With this question the respondents took their time to and named their various first impressions. They were unanimous in saying that it was quite comprehensive. That there was a lot of information. One found the information to be displayed in a clear way, another found the website lacking in clarity. The division of the information into a menu was named "*very useful*" (Interview Ilona 2011), but Jan pointed out that none of the options was to see what information was actual. What information was recent. The general first impression was one of an extensive information source in which one was supposed to find their way.

Because the respondents were asked to visit a website that could stimulate their safe use of the internet, they already knew it to be a website that was aimed at just that. Adding that it was a website from the government made them not question the validity of the information. They assumed it to be correct. One respondent cleverly pointed out that one was stimulated to check the Internet location (URL) of websites. And as the website was moved to another URL after the campaign ended (but was still available from it's old URL) one could doubt whether one was at the right Internet location. The respondents were asked to visit www.veiliginternetten.nl, but that URL redirected the user to www.nederlandveilig.nl/veiliginternetten. The old Internet location is not used anymore in communication by DPC (Interview de Jong, campaign manager, 2011), but is still used by ECP-EPN, as can be seen on the Digivaardig & Digibewust website. That the user was asked (by the website) to check if they are at the right website resulted in a clever observation from Marije: "*That happens with banks and is so stupid! They change their website every now and then! They say that if you recognize the site you're at the right location, but changing the appearance of websites makes them unrecognisable!*" But the awareness of deceptive Internet pages and testing them against their URL was passed on.

The animations were the first to be viewed by all respondents. Not only were they viewed, they named one 'tip' that remained with them. For Wil, this was 'changing your password'. Although she was the one who used Internet the least, and even has no personal information on the Internet at all, she was familiar with passwords and that they were important. The three other respondents all mentioned that from now on, they are watching the 's' behind 'http'. The animations however, also raised questions. Wil had a password on her entire system, installed for her by an IT specialist. She wanted to change her password, but didn't know how to. Upon watching the animation with the tip to check who you send your personal information she gave a similar reply: "*Check who you send your personal information to. OK. But how do I do that?!*". An equivalent response from the more IT knowledgeable respondents was the difficulty of remembering passwords. They acknowledged that changing passwords was stimulating their safe Internet use. But they were reluctant to change their current ones as they didn't know how to create easy to remember, but hard to guess passwords. The animations had a surprisingly positive inviting effect on the users.

The interview continued by asking what they did with the website. And here the respondents shifted in various directions. The elderly woman said that she didn't use the website after seen the homepage as none of the articles related to her Internet use. The three Internet users who did use Internet for more purposes all looked up additional information on the tips. Marije continued with reading the "what is...?" section, to inform herself on the various dangers of internet. Jan directly went to do the test to see what 'digitype' he was. Then he tried to see if there was information that was applicable to his company. Ilona went through the entire website, enlightening herself on all government activities and it's partners. "*I'm glad the government is doing so much. That's a comforting thought.*" After seeing the animated tips, the use of veiliginternetten.nl was strongly influenced by the extent users take interest in cybercrime, and quickly disregard everything that does not relate to their particular Internet use.

Upon designing the campaign, DPC had to keep in mind that users should not be discouraged or become scared when being confronted with the risks and dangers of internet. "*That's quite hard. Because you don't want to instil too much fear. It's also not the case that in reality, everyone is being hacked, or has information stolen*" (Interview de Jong, campaign manager, 2011). With Marije, exactly this happened. As the website contains so much information on the topic of cybercrime and it's effects, she got nervous when using the website. Even uncomfortable when reading what could happen to you just by using the internet: "*A back door. I found that frighting. That someone can just take control of your computer.*" She compared reading the various risks of Internet use by a police officer telling you in what nasty situations you could end up when walking on the street. There were more reactions that concerned people's awareness of cybercrime. But only Jan, the entrepreneur, said that cybercrime seemed 'closer' now that he read about it. Clearly, even among the small group of respondents, I found a great variety in the way, the script of veiliginternetten.nl was "read". One user was overwhelmed by the possible dangers, whereas another one users rather de-scripted the website' script as providing a sense of security now that she knew the government was so extensively working on it.

Now that the respondents were provided with information on cybercrime, I asked them if they carried out specific acts or used Internet differently. Most respondents said they are now watching the 's' behind 'http' was the most mentioned act of safety. Another change in behaviour was keeping track more often of the Internet location while browsing on a website. The ID-Alert was ignored by one, and in two cases let to a Google search on their own name. They did not however, activate the alert. The optician updated a software program on her computer, and the entrepreneur checked the contracts he had with IT service companies. The elderly woman wanted to change her passwords, but she had no idea how to realize this.

By analysing the actual use of the website different uses and approaches have been found. And the combined analyses of all four respondents give a rich picture of the user logic of veiliginternetten.nl. The website shows inviting behaviour (animations) as well as inhibiting behaviour (search for information). There are also different effects upon use, which were not intended upon inscription (delegating responsibility to the government rather then the Internet user). With these findings in mind, I can compare the different aspects of the script of veiliginternetten.nl.

6.4 Making and breaking the script

By approaching the script from veiliginternetten.nl from three angles, there are various discrepancies to be found among them. I will outline these using the tensions found in the network of involved actors, as described in chapter 4. These were the different views on veiliginternetten.nl between DPC and the Ministry of Justice, between the Ministry of Justice and Economic Affairs, and between DPC and ECP-EPN.

The first tension entails the way the user was to be informed on cybercrime. Or: the message that was to be sent to the user. The Ministry of Justice wanted a broad range of information on the subject to be present on the website. Next to the central one, firstly personal information and secondly online transactions, the user was also invited to inform him- or herself on a broad range of other topics concerning cybercrime. This includes the technical shortcomings, but also the additional information that the government was to provide help, and in what way. DPC, on the other hand, wanted short, simple and clear messages that would stick in people's mind. The result of this tension was found in veiliginternetten.nl's script that invited the user not only to watch the short and simple tips, but also invite the user to find out what other risks and threats were present in Internet use. Including a whole variety of threats that could not be applicable to the user. Secondly, by sending the message that the government was working on cybercrime with many parties, the message that the user should be responsible for it's own safety became ambiguous. Resulting in the answers given by all real users that the website contained “a lot” of information, and provided too much information the real user couldn't use. Furthermore it was pointed out by Ilona that it was “*a pleasant thought that the government did so much against cybercrime*” and all users replied that their personal responsibility was only stimulated in a very small way. The script of veiliginternetten.nl was not a short and simple one.

A very striking discrepancy found in the script analysis was the accuracy of the inscription process and the de-inscription by the user towards the way in which they would inform themselves. However this part of the script was not found in the actual script of veiliginternetten.nl. Namely that Internet use differs among the broad range of users, and they subsequently look for information applicable to their particular situation. This was inscribed into the website using the different points of entry into a topic, which the real users acted out by looking for information regarding their child and their company. But as veiliginternetten.nl did not contain a search function, and inhibited the user to navigate the website by navigating them away to external locations, this part of the script did not facilitate this anticipated and actual use of the website.

The second tension, between the two different ministries, was also found in the script analysis. The Ministry of Justice took an interest in reducing cybercrime and focused on the personal information that was exploited. This was however not subsequently inscribed into veiliginternetten.nl and also not de-inscribed by the real users. When the topic changed and the Ministry of Economic Affairs was added to the network, the central topic was again not inscribed into veiliginternetten.nl. As so much other information was inscribed into veiliginternetten.nl (also seen in the first tension), implying that the central message conveyed to it's users became rather vague. Should users protect themselves to reduce crime? Should the users conduct safe transactions to utilize Internet for trade? The topic became ambiguous.

Real users de-inscribed veiliginternetten.nl predominantly as to stimulate safe transactions. The 's' behind 'http' and watching URLs in general was mostly seen as most useful contribution to their Internet use. But the website's script also has various external links to collaborators of the Ministry of Justice. These have been inscribed into veiliginternetten.nl and are subsequently inviting the users to visit their Internet locations to report crime or theft. The real users however did not de-inscribe it as such. Three of the four respondents did not visit external locations, but would only visit them if they had a problem, and wanted to reduce cybercrime. Due to the unclear goal in the script of veiliginternetten.nl, Ilona even pointed out after reading a good deal of all available information that it was not particularly clear what the website was for, but that she found the tip on the 'https' to have “*her learned something after all*”.

The last tension resulted in the ambiguous script that could invite the user to either further their safety online, or further their abilities to work with computers and the Internet in general. Wil, the elderly woman, was not attracted by the aspect of online safety, but was attracted to the notion of using difficult passwords. As she didn't have online personal information or transactions protected with a password, but did have her computer protected with a password, she was now educated into general computer use. This might be a positive development, it was however not the goal of veiliginternetten.nl. By adding to the website the efforts of ECP-EPN, veiliginternetten.nl also resembled a technology applicable to computer use in general and was hence as such de-inscribed by someone who described the website as not applicable to her as Internet user.

The ID-alert is a similar part of the script that does not protect users against risks or threats of internet. Inviting the user to use an application on the Internet that monitors if information is published using their information, is rather asking them to be engaged with the possibilities of internet. Real users de-inscribed it in a similar way and did not use the ID-alert. They did not see how using such an application would protect them from harm on the internet. It did do something else though. Now that users were informed that they could look up information about themselves, two users looked themselves up in a search engine: "*Ye I liked that. I thought, let's Google myself to see if something comes up. But there was nothing noteworthy about me, so I'm happy about that!*". The last tension in the network made veiliginternetten.nl resemble partially an informative website on computer- and Internet use in general.

By applying a script analysis, I've shown how the discrepancies between the various stages of a script bring insight into the workings of this technology. I've analysed how the designers have inscribed their constructed user, and the resulting script. And how the technology is subsequently used by real users. And although the inscribed use greatly resembled the actual use, the script analysis into the website itself has made visible the discrepancies that led to different effects on the users. Now that the final part of the research has been done, I will summarize how the network, users and scripts of veiliginternetten.nl relate to safe Internet behaviour.

7. Conclusions and recommendations

My research asks the question how a website can contribute to safe Internet use. I've approached this question by providing a look into the current knowledge on Internet safety and user awareness, and performed a case study using a script analysis. The veiliginternetten.nl website was designed to stimulate the safe Internet use of the Dutch public, and should hence be appealing to an enormously large audience. The goal of veiliginternetten.nl was to change behaviour in such a way that the Dutch public should be more aware of the risks and dangers of Internet use, and be provided simple tips and tools to do so. In my research I've taken this website to be a technology. One that was designed with a constructed user in mind. I analysed the website from an STS point of view to see how this website could change behaviour. This chapter outlines the conclusions and recommendations.

By analysing the design and use of the veiliginternetten.nl website, my findings show how discrepancies in agenda's and interests of the different involved parties can result in an ambiguous design with a subsequent diversity of effects upon use. Next to this, the design could have been adjusted more to the knowledge present at the designers. The findings show that this knowledge on the use of the website was very much in line with the actual use. And as the constructed user was "configured as everybody", the real user shows why users approach (de-inscribe) veiliginternetten.nl differently, but with the website prohibiting this diverse range of approaches.

Diverging interests and agenda's of stakeholders results in an ambiguous design

The group of involved actors as I described in chapter four show tensions in the shape of veiliginternetten.nl. There were quite a number of actors who had their influence in the resulting website. By describing these tensions, I showed how these different expectations led to an ambiguous design. The website incorporated the tension between an information source and simple message; between a technology to prevent cybercrime and a stimulant for the market; and between a tool for safe Internet use and Internet use in general. This was seen by the reaction from the respondents who were discouraged by the sheer amount of information. Similarly, the elderly woman was stimulated to work on passwords, of which she had none relating to Internet use. While other real users were stimulated to check for secure websites (which have the 's' behind 'http'), which does relate to safe Internet use. But the tensions did not only result in these different uses of veiliginternetten.nl.

Another ambiguity arising from the extensive network was seen in the way the website raised awareness. Stimulating safe Internet use can be divided into two categories: raising awareness that one's online safety lies with themselves, and providing tips and tools to use Internet safely. Veiliginternetten.nl did a good job in meeting the second aspect by providing simple tips that all users picked up by looking at short animation clips ("*I should really change my password!*"). But the website proved to induce very different results when trying to raise awareness. This intended goal was seen in one respondent who was reminded that one should be careful. Another respondent however, was discouraged on the subject by reading all the dangers, and yet another was glad the government was working on the problem. The last respondent did not even perceive the whole awareness to be applicable to her. Making the component of user awareness have very ambiguous results.

Here I need to refer to the other online means to raise awareness and the campaign as a whole. The campaign also included TV- and radio commercials, as well as the Market Place takeover and Hyves viral. The results from the research indicate that the aspect of raising awareness should be delegated more to the other products of the campaign ("*they got the message*"), and the aspect of providing tips and tools should be emphasized in the website. Of the four respondents, all but Wil would visit veiliginternetten.nl again if they actually had a problem, assuming the website would remain available online as informative source on the subject of cybercrime.

To overcome the obstacles arising from a diverse range of expectations towards the website, one could of course limit the amount of involved actors and/or their influence. But better yet, one could look at the delegation to, and design of, the artefacts that are to be used for the purpose of educating the public. The research shows that short simple animations "*stick in people's minds*", and that a large cumbersome website prohibits engagement with the subject of cybercrime. Similarly, the research showed how this extensive range of expectations resulted in an ambiguous website. And the intended goal to stimulate awareness and provide simple tools merged into one pool of text that can't be distinguished in importance or relevance. Moving secondary information to the bottom of the website, or in a smaller font or colour, can help users distinguish between the primary objective of the website, and the additional information.

The in-depth look into the envisaged use and actual use of the website reveals a mismatch

The most notable conclusion arising from my analysis is that although the anticipated use of the website by DPC was rather in line with the actual use by the real users, the script from veiliginternetten.nl does *not* facilitate this use. The briefings show an anticipated use by informing the user on a particular risk, when this risk is applicable to the user, what the symptoms are, and what the user can do about it. This example of envisaged use was indeed applied by the real users, however none of the risks described on veiliginternetten.nl was actually in this format. Subsequently real users could not work out how to deal with a problem ("*Check who you send your online information. OK. But how?!*"). Or work out why it would be applicable to their particular behaviour.

Likewise, it was stated in the briefings that users could look up specific information. And from a search function should be redirected towards that particular risk described in the aforesaid aspects. Looking up certain aspects of Internet safety was done by the real users, but the website did not include a search function, and inhibited the users from looking up more information as they were redirected to other parts of the Internet without the option to return to veiliginternetten.nl. A (simple) search function would invite the users to quickly look up information specific to their needs.

Another discrepancy between what was inscribed into the script and it's actual use was the actuality of information on cybercrime. Cybercrime was defined as (quickly) changing over time. In the first briefing it was stated that the information provided on veiliginternetten.nl was to be actual. That it had to provide updated information. The entrepreneur acted in just such a manner and was missing recent information on Internet safety. Just as the mother could not find information regarding the use of Internet by children. Future websites that aim to stimulate safe Internet use could benefit from methods to keep the user interested. "*Instead of serving as one-shot repositories of safety tips, online interventions might encourage repeat visits to build self-efficacy and maintain action control*" (LaRose 2008). Online interventions like listing weekly updated publications on cybercrime, or send a monthly e-mail to inform the recipient on new insights into a topic of their choice. And to more align certain risks and dangers with the particular use of the user has another reason.

Configuring the user as everybody is indeed problematic

The differences between anticipated use and real use is amplified by the discrepancies between the constructed user and real user. Real users only concern themselves with their particular angle towards cybercrime, but the website was created as if all Internet users are the same. A user that uses Internet for the same multitude of applications. Real users, even taken from (only) four individuals, already show such a wide variety of stances towards cybercrime that their individual questions were not satisfied by the general approach found in veiliginternetten.nl.

The most notable example of this difference is found in the Internet use of Jan and Ilona. Their Internet use differs so greatly that it becomes very hard to design one website that would appeal to them both. Whereas Jan uses Internet nearly exclusively for work related purposes on his company computer and network, Ilona uses Internet almost always at home for private purposes. Also Marije and Wil show how qualitative research reveals great discrepancies between Internet use. Wil does use Internet for multiple purposes, but this is only a small subset of the great variety of purposes Marije uses the Internet for. By configuring the fictive user as everybody, all these different ways in which Internet is used, and what for, is reduced to a small set of practices. Knowing what the user would deem important and where the user can be stimulated into a more safe use of the Internet then becomes a very problematic task.

Also the answers given by the real users towards their attitude reveal problems for creating a website for everybody. Both Ilona and Marije have ICT knowledgeable relatives. For these two women there is very little reason to fervently occupy themselves with the risks and dangers of Internet use, and the protective measures ("*If the computer caught a virus, then my IT friend fixes the problem*"). The constructed user might want to be informed and stimulated in their responsibilities towards Internet use, this example of the real user shows how futile such a conscious raising effort might be.

To overcome these obstacles there also options to take into account when designing the website. Apart from the search function, prior research already indicated that creating means for users to indicate their interests is a good idea: "*User education Web sites could screen visitors with "i-safety IQ" quizzes that would route them to appropriate content*" (LaRose et.al. 2008). Next to a quiz, technically functioning as routing system towards specific content, the designers could also follow classifications like I did. By dividing Internet users into entrepreneurial, parents with children, the elderly and the digitally illiterate (average user), veiliginternetten.nl could display four buttons or pictures and have the user of the website choose one of them, resulting in a different collection of risks, tips and tools particular to their interests.

In conclusion, the change in safe Internet use by using the veiliginternetten.nl website turns out to be ambiguous. From a large and extensive network a technology was designed that had to incorporate many informative aspects and had to appeal to a very large user group. Findings show that the real users did have a change in their awareness, but it ranges from the intended goal (thinking about Internet safety) to thinking the government would work on the problem, to having a discouraging effect to become more aware of the current risks associated with Internet use. Likewise, real users did find relevant tips and tools that can be added to their protective measures. However there are also risks, tips and tools out of reach of the real user, as they were inhibited to search or let the website in some way know what their topic of interest was. Veiliginternetten.nl did have a positive effect on their users, but also proved to be ineffective in doing so.

The analysis makes for a contribution to the ongoing efforts to educate Internet users on Internet safety. The Safe Internet Use campaign from the Ministry of Safety and Justice was a successful one (Interview de Jong, campaign manager, 2011) and findings do show an increase in user awareness and in the user's means to do so. But future efforts could benefit from a more unanimous approach from it's designers to the design, and incorporate more utility to appeal to a more individualized safe use of the internet.

7.1 Further research

DPC is not the first to delegate user awareness and informing the Internet user to a website. These websites have been around longer, and are still made today. The most recent one comes from Google (Google Good to Know 2011). Similarly, the effects of these campaigns are also still reflected upon. Not in the least by the designers themselves for evaluation. But also by the academic community. "*Still, much work needs to be done to better understand online safety behaviour, including experimental studies that can validate the causes of both safe and unsafe behaviour*" (LaRose et.al. 2008). My research gives an overview of different factors that play upon designing such a website. When delegating a stimulant in behaviour to a website, my script analysis reveals how inscribed user representations can lead to different approaches to such a website from the real users.

The findings of this thesis also show how a website is just among many means to raise user awareness, but these means can complement each other well. For example, the other online means to stimulate user awareness from the Safe Internet Use campaign show how they can be helpful in designing a user awareness website. By making websites that would pop up during visits to other websites like the Hyves viral and MarketPlace takeover, the user was not only invited to learn more about cybercrime, the very notion that it popped up already made the Internet user think about the safety aspect of Internet use. Srikwan et.al. (2008) also tried delegating this to cartoons. And not just the means, but also the message the technology is to convey can change. Jelsma (2006) asked how to design a moralizing product. His 'message' showed great resemblance to mine (government wanting to stimulate behaviour for the 'greater good'), and websites or other online means can very well incorporate other messages aimed at stimulating or counteracting certain behaviour. As many of these campaigns place such an emphasis on the user (Jelsma 2006) research could be done into the creation of the right artefacts to stimulate behaviour, "*rather then placing the onus of discovery on the individual*" (Furnell et.al. 2006).

Lastly, my research contributes to the ongoing argument that users matter (Oudshoorn & Pinch 2003) as do non-users (ibid, and Wyatt 2003). This research indicates that the way an envisaged user is incorporated into the design of an artefact stimulates and constrains the actions of their users. By providing qualitative interviews, I got a picture of the 'why' of safe Internet use, as opposed to the 'what' question of quantitative interviews. The elderly woman's notion that one should not use technologies one does not understand, shows an example of what happens to the non-user. With a growing understanding of this interaction between websites and their users, designers of websites can benefit from these recent insights to steer the user into a more safe Internet use.

7.2 Reflection

A master thesis project is limited in time and resources. Not all actors involved in the actual creation of the website could be interviewed. In the design context I focused on the level of policy makers and not so much on the actual designers. The actual design of veiliginternetten.nl involved at least four different organisations: one company designed the outlook of the website, an ICT company implementing the website, and two other companies created specific components like the test and the film clip. Time constraints also limited the analysis of the user representation techniques. As I used primarily the results from the market surveys my analysis has mainly focused on the "explicit techniques", leaving possible implicit representation techniques out of scope. The question to what extent implicit techniques were used and how these techniques possibly shaped the script of veiliginternetten.nl can only be answered if the designers and programmers would have been interviewed.

7.3 Acknowledgements

I would like to thank Jan, Wil, Ilona and Marije for their willingness and participation. I'm grateful for their cooperation and the interviews I held with them. I also would like to thank mw. De Jong and dhr. Krenn for their time to partake in the interview.

Secondly I would like to thank my supervisors for their guidance, support and feedback during writing. Notably Ellen van Oost who gave many in-depth and constructive comments.

8. References

Akrich, M. & Latour, B. (1992) *A summary of a convenient Vocabulary for the semiotics of Human and Nonhuman Assemblies*, in: Bijker & Law (1992) Shaping Technology / Building Society, p.259-264.

Akrich, M. (1992) *The De-scription of Technical Objects*, in: Bijker & Law (1992) Shaping Technology / Building Society, p205-224.

Akrich, M. (1995) *User Representations: Practices, Methods and Sociology*, in: Rip, A., Misa, T., Schot, J. (eds.) Managing Technology in Society. The approach of Constructive Technology Assessment. Pinter, Londen / New York, pp.167-184.

Callon, M. (1986) *The Sociology of an Actor-Network: The Case of the Electric Vehicle*, in: Callon, M et.al. (1986) Mapping the Dynamics of Science and Technology p.19-34.

Cormode, G. (2008) *Key differences between Web1.0 and Web2.0*, First Monday, Volume 13, Issue 6, pp. 1-30.

Cranmer, S. et.al. (2009) *Exploring primary pupil's experiences and understandings of 'e-safety'*. Springer Science + Business Media, Educ Inf Technol (2009) 14:127-142. DOI 10.1007/s10639-008-9083-7.

Furnell, S. et.al. (2008) *Who guides the little guy? Exploring security advice and guidance from retailers and ISPs*, Computer Fraud and Security, p.6-10.

Furnell, S. (2010) *Hackers, viruses and malicious software*, in: Jewkes, Y. and Yar, M. (2010) The Handbook of Internet Crime, pp. 173-193, Willan Publishing, UK.

Gauntlett, D. (2004) *Web Studies: What's New?*, in: Gauntlett, D and Horsley, R. (eds), Web.Studies (2nd edn). London: Hodder Arnold.

Görling, S. (2006) *The Myth of User Education*, Virus Bulletin Conference.

Grazioli, S. (2004) *Where Did They Go Wrong? An Analysis of the Failure of Knowledgeable Internet Consumers to Detect Deception Over the Internet*. Kluwer Academic Publishers, Group Decision and Negotiation 13: 149-172.

Jelsma, J. (2006) *Designing 'Moralized' Products: Theory and Practice*. in: Verbeek, P.P.C.C. & Sloc, A. (eds.) User Behaviour and Technology Development: Shaping sustainable relations between consumers and technologies. Springer, Verlag, pp.221-231.

LaRose R. et.al. (2008) *Promoting personal responsibility for Internet safety*, Communications of the ACM, v.51 n.3, p.71-76, March 2008

Lasilla, O. and Hendler, J. (2007) Embracing “Web 3.0”, IEEE Internet Computing, Volume 11, no. 3, pp. 90-93, May/June 2007, doi:10.1109/MIC.2007.52

Latour, B. (1992) *Where are the missing masses? The Sociology of a Few Mundane Artifacts*. in: Bijker & Law (1992) Shaping Technology / Building Society, p.259-264.

Nelson, T.H. (1965) *Complex information processing: a file structure for the complex, the changing and the intermediate*, in: Proceedings of the 1965 20th national conference, pages 84-100, ACM Press, New York, USA.

Oudshoorn, N. and Pinch, T.J. (2003) *How users matter: the co-construction of users and technologies,* MIT Press, USA.

Oudshoorn, N. and Somers, A. (2006) *Constructing the digital patient. Patient organizations and the design of health web sites*. Information, Communication and Society 5.

Oudshoorn, N., Brouns, M. and van Oost, E. (2005), "*Diversity and Distributed Agency in the Design and Use of Medical Video-Communication Technologies*", in: Harbers, Hans (ed.) Inside Technology. Agency and Normativity in the Co-Production of Technology And Society. Amsterdam: Amsterdam University Press, 85-105.

Oudshoorn, N., Rommes, E., Stienstra, M. (2004) *Configuring the User as Everybody. Gender and Design Cultures in Information and Communication Technologies*, Science, Technology & Human Values, January 2004, vol. 29, no. 1 pp. 30-63.

Platt, D.S. (2007) *Why Software Sucks...and what you can do about it*, Addison Wesley, USA

Punie, Y. (2000) *Domesticatie van informatie- en communicatietechnologie. Adoptie, gebruik en betekenis van media in het dagelijks leven: Continue beperking of discontinue bevrijding*? Proefschrift Vrije Universiteit Brussel, Juni.

Quayle, E. (2010) *Child Pornography*, in: Jewkes, Y. and Yar, M. (2010) The Handbook of Internet Crime, pp. 343-368, Willan Publishing, UK.

Rommes, E. (2002) *Gender Scripts and the Internet. The Design and Use of Amsterdam's Digital City*. PhD Dissertation University of Twente, The Netherlands.

Rommes, E., Oost, E. van, and Oudshoorn, N. (1999) *Gender and the design of a digital city*, Information, Communication and Society 2, 4:476-95.

Sharples, M. et.al. (2009) *E-safety and Web2.0 for children aged 11-16*. Journal of Computer-Assisted Learning, 25, 70-84.

Siponen, M.T. (2001) *Five dimensions of Internet security awareness*, ACM SIG CAS Computers and Society, 21, 2 (2001), 24-29.

Solms, R. von (1999) *Information Security Management: Why standards are important*. Information Management & Computer Security 7/1 [1999] 50-57, MCB University Press

Srikwan, S. et.al. (2008) *Using cartoons to teach Internet security*, Cryptologia, 32:137-154, Taylor & Francis Group, LLC.

Stanton, J.M. et.al. (2005) *Analysis of end user security behaviors*, Computers and Security 24, 2(2005), p.124-133.

Verbeek, P.P.C.C. (2005) *What Things Do*. The Pennsylvania University Press, USA.

Wyatt, S. (2003) *Non-users also matter: The construction of users and technologies,* in: Oudshoorn, N. and Pinch, T. (2003) *How users matter: The co-construction of users and technologies,* pp. 41-56, The MIT Press, USA.

Wykes, M. and Harcus, D. (2010) *Cyber-terror: construction, criminalisation and control*, in: Jewkes, Y. and Yar, M. (2010) The Handbook of Internet Crime, pp. 214-229, Willan Publishing, UK.

8.1 Internet Resources

Digivaardig & Digibewust, Retrieved November 2011 at http://www.digivaardigdigibewust.nl/

Veilig Internetten | Nederland Veilig, Used and visited during 2010-2011 at http://www.nederlandveilig.nl/veiliginternetten/

IWS (Internet World Statistics) *Internet Usage Statistics: The Internet Big Picture*, Retrieved December 2011 at http://www.internetworldstats.com/stats.htm

Google Good To Know, Retrieved January 2012 at http://www.google.com/goodtoknow/

Microsoft Safety & Security Centre, Retrieved at January 2012 at http://www.microsoft.com/security/

ING veiligheid, Retrieved January 2012 at http://www.ing.nl/particulier/klantenservice/veelgestelde-vragen/internetbankieren/mijn-ing-met-gebruikersnaam-en-wachtwoord/veiligheid/

Safer Internet Programme: Empowering and Protecting Children Online, Retrieved May 2011 at http://ec.europa.eu/information_society/activities/sip/index_en.htm

8.2 Resources Dienst Publiek en Communicatie

DPC, Intomart en Daphne (2008) *Campagne 'Cybercrime' (K09) Rapportage Vooronderzoek*, Ten behoeve van het Ministerie van Justitie, Projectnumber: PK09R1, October 2008.

Intomart GfK bv (2008) *Cybercrime*, Rapport focusgroepen met burgers in opdracht van het Ministerie van Justitie, Projectnummer: 18297, 18-12-2008.

Dienst Publiek en Communicatie (2009) *Briefing Cybercrime*, auteur: L. Bourgonje, 6 May 2009.

Daphne (2010) *Eindrapportage Veilig Internetten*, Management Summary, (L07) August 2010.

8.3 Interviews

de Jong, P., campaign manager at Dienst Publiek & Communicatie, Ministry of General Affairs

- Personal interview: 26 July, 2011.

Krenn, M., online advisor at the Ministry of General Affairs

- Personal interview: 26 July, 2011.

Hartel, prof. dr. P.H., professor of Cyber-crime Science, University of Twente

- Personal interview: 20 April, 2011.

Kranenburg, J. van, CEO of ERT in Deventer

- Personal interview: 19 July, 2011.
- Personal interview: 25 July, 2011.

Wiltink, I., receptionist at 't Centrum in Twello

- Personal interview: 12 July, 2011.
- Personal interview: 26 July, 2011.

Kuijk, M. van, optician at Hans Anders in Deventer

- Personal interview: 18 July 2011.
- Personal interview: 25 July 2011.

Klosters, W., retired, living in Schalkhaar

- Personal interview: 5 July 2011.
- Personal interview: 11 July 2011.