Risks and benefits of online privacy in single sign-on systems

Name: Milou Gijsbers
Registration nr: 900608290010
Date: June 2015
Place: Wageningen University
Content: MSc Thesis
Supervisor: Arnout Fischer
Second reader: Ellen van Kleef
Course code: MCB-80433

Table of Contents

Abstract

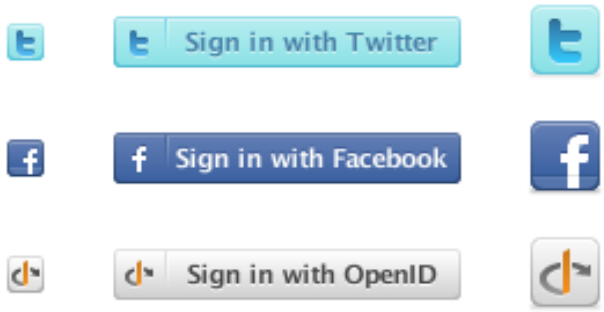
Nowadays internet users have multiple passwords for multiple accounts which is not very convenient. A possible solution for this problem is using single sign-on systems. Single sign-on systems are systems with which people can login to multiple accounts with only one password. Besides the convenience of having to remember only one password, these single sign-on systems also bring along some privacy risks. This study investigated the influence of single sign-on systems on risk perception and benefit perception.

This study investigates what influences the risks and benefits of using a single sign-on system and how people make a trade-off between the risks and benefits in order to make a decision whether people have the intention to adapt a single sign-on system. An experiment showed that people experience a general-economic risk and a psycho-socio risk and having one password as main benefit. One password seems not only to influence the benefit perception but also the general-economic risk perception, which lead to a trade-off and final decision

1. Introduction

Online social networks like Facebook, Twitter, Instagram and MySpace are popular ways to stay in contact with your friends. We are able to share what we are doing, where and whenever we want. Facebook is still the leading social network, although the number of users is decreasing since 2013 (Newcom research & Consultancy, 2014; Statista, 2014). Nowadays Facebook can be linked to almost every website, platform and other third-parties apps. Facebook Connect is a Single Sign-On system with which internet users can easily create an account or profile on third-party apps and websites, it only needs two clicks (Bauer et.al., 2013). This way a lot of our online activities are linked to our Facebook account. Other single sign-on systems are OpenID and Twitter and can be recognized by the login buttons as shown in picture 1.

Picture 1. Single sing-on system buttons



Along with the benefits of social networks and single sign-on systems come privacy and security concerns (Govani & Pashley, 2005; Acquisti & Gross, 2006). People post personal information on social networks which might be seen by people or organizations we do not want it to see. Facebook and fellow Facebook users are not the only one who have access to your personal information, also advertisers (indirectly) and third-party apps (Besmer & Lipford, 2010).

In the situation where users are able to create a new account they can choose between visiting the website or app without an account, making a new account or link it to his Facebook account, which already contains the information that is needed for a new account. Here the user can benefit by choosing to link this new account to his Facebook account, which takes less effort than making a new account. The cost for disclosing information through linking new accounts to one's Facebook account is a privacy risk. People base their decision to disclose personal information on the *privacy calculus*, a cost-benefit analysis which weighs the benefits in relation to the privacy costs (Laufer & Wolfe, 1977).

The problem in this situation is that users give away a lot of personal information and thereby risk their privacy, while they do not get much in return. In the situation described above it seems that users perceive it worth the risk to disclose information in return for an easy way to make an account. Even though internet users are concerned about their privacy and the security of their personal information, they choose convenience over this privacy concern (Acquisti & Gross, 2006). This leads to the question: *How do internet users perceive the risks and benefits of linking new accounts to existing accounts and do they make a trade-off in order to make a decision.*

Therefore the purpose of this study is to investigate why internet users give away their privacy without gaining relatively little benefit. In order to find these reasons there are a couple of things

that need to be clarified. First we look at whether users do actually perceive privacy and security risks. Second it is important whether internet users perceive benefit. Last we need to know whether internet users do actually make a trade-off between the costs and benefits in this situation and how this trade-off is done. This leads to the following research questions:

- *What risks do internet users perceive when linking new accounts to an existing account?*
- *What benefits do internet users perceive when linking new accounts to an existing account?*
- *Do internet users make a trade-off between the benefits and costs of linking existing accounts to a new account? If so, how?*

When these questions can be answered, this will explain how much benefit and risk users perceive and whether they make a trade-off between these perceived benefits and costs. This will explain why people do link their online accounts to their Facebook account so easily. When we know why people behave in this way, we have a better understanding of the perceived benefits and risks in this situation. In a scientific way, this research adds new insights to the literature about why internet users perceive it worth the risk to disclose information in return for an easy way to make an account.

To answer these questions there will be a literature study on the existing knowledge for these three questions in chapter 2. The findings of the literature study will be empirically tested.

2. Literature

2.1 What risks people perceive when disclosing privacy

Previous studies show that internet users are concerned about their privacy and the security of their privacy online (Acquisti & Gross, 2006; Young & Quan-Haase; Krasnova et. al., 2009). People are concerned about the extensive amount of collected information that is stored in databases. Internet users can also be concerned about their privacy because of different risks. Privacy risks arise when people feel that they are not in control over the personal information they disclose (Westin, 1967). Because people give their privacy away, they are not in total control of it anymore and then it comes down to trust in the party that has one's personal information.

Risks of linking accounts

Risk is a situation of uncertainty for the possibility of a negative outcome (Oxford dictionaries, 2014; the Free Dictionary, 2015). A negative outcome can be harm or losing something of value. In general seven types of risks can be identified: financial, performance, physical, psychological, social, time, and opportunity cost risk (Jacoby & Kaplan, 1972). When people link new accounts to existing accounts, the provider of the new account gets access to the available personal information of the existing account. This means another party has access to the personal information. In a situation of linking new accounts to existing accounts, the perceived risk does now depend on two online actors. This section contains an evaluation of what risks people perceive when they link a new account to an existing account.

In the case of disclosing personal information, there are three relevant possible risks; a psychological risk, a social risk and a financial risk. These three risks have been associated with risks in online environments (Forsythe & Shi, 2003). A social risk is the probability of other's unfavorable thinking, about the disclosed information (Lee & Stoel, 2014). In general disclosing personal information is associated with perceived social risks because of possible negative social outcomes, for example when personal information is abused which leads to bullying or stalking. The social risk does apply in the situation where people use a single sign-on system, because people are concerned about how others perceive their personal information and what consequences this has for example for their social status (Crespo et.al, 2009).

A financial risk can be defined as the uncertainty of a possible monetary loss (Biswas & Biswas, 2004). Disclosed information might in some cases contain one's personal banking information. When this personal banking information comes in unwanted hands, this could mean a monetary loss. Therefore it is possible that people perceive financial risks in situations where financial information is involved in the linked accounts. The level of the perceived risk is dependent of the website category that is involved (Bart et.al.,2005).

The psychological risk in the online environment refers to the possibility that one's privacy is violated which might result in disappointment, frustration, and shame (Forsythe & Shi, 2003). A psychological risk can be the result of a negative result of the social risk or financial risk. For example the social risk might go hand in hand with a psychological risk when the negative results of the social risk have a negative effect on a person's self-perception and self-esteem (Mitchell, 1992). Also the negative outcomes of the financial risk could lead to disappointment, frustration and shame. Therefore the financial risk could also lead to a psychological risk.

Risk situations

There are three explicit situations in disclosing personal information that might result in financial, social and psychological risks (Smith et.al., 1996). There is *unauthorized secondary use,* which can be internal or external. This is the concern for the risk that collected information is used for secondary purposes without permission. Here, internet users perceive threats from organizations and third parties that make use of personal information for example for marketing purposes (Krasnova et. al., 2009). Second, *improper access*, this is the concern that unwanted people might have access to one's personal information. This could be external people that gain access in an illegal way, or people within the organization that do not have the 'need to know', for example employees that do not necessarily need to know should not have access to it (Smith et. al., 1996). This could lead to identity theft or social threats like bullying and stalking (Krasnova et. al., 2009). Another risk is that the protections against deliberate and accidental *errors* in personal information are inadequate. This is related to the data quality which should ensure the accuracy of the personal information (Smith et. al., 1996). In all these situations there is a risk that one's privacy is violated which could negatively result in financial, social and psychological damage. These risk situations are possibilities of how personal information could be violated. This study assumes that internet users do not make a difference between these situations, because they feel the overall concern of privacy risks. Therefore these risk situations are not measured or included in the model.

Perceived risk

The extent to which a person experiences risks does depend on one's risk perception. For the perceived risk the perceived impact (negative outcome) is weighted by its probability of occurrence (Tversky & Fox, 1995). This means that when a person perceives a high risk in a situation of disclosing personal information, this person thinks it is very likely that this information will be misused.

There are four categories of trust antecedents that influence the perceived risk in an online environment: cognition-based, affect-based, experience based and personality oriented (Kim et.al., 2008). These four categories are based on consumers' perceived risk in a context of electronic commerce, which is comparable to online users who disclose personal information in order to gain something.

The *cognition-based* category includes the perceived privacy and security protection, system reliability and information quality (Kim et.al., 2008). These antecedents are based on people's observations and perceptions of privacy protection and system reliability. These observations rely on a person's knowledge about the single sign-on system and the third party that will receive the personal information. These antecedents apply to the situation where personal information is stored in databases, on which people have to trust the security protection and the reliability of the system that holds personal information. When people trust the single sign-on system based on their observations and perceptions, their risk perception decreases (Kim et.al., 2008). The observations and perceptions of whether to trust the single sign-on system or not, could be influenced by whether people are familiar with it or not. Other studies show that even though people show concerns about privacy and data-sharing, they are unaware of audit tools that are provided by identity providers. Also the information that is shared by identity providers is not understood by people, because they are based on preconception, even though the content of informational dialogs was displayed (Bauer et. al., 2013; Egelman, 2013). This means that displaying this information does not decrease the

perceived risk. Even though displaying the content of informational dialogs does not decrease the perceived risk, it is assumed that when the information is available this makes the third-party more reliable than when it was not displayed. This means that the observations and perceptions of privacy protection and system reliability are not influenced by displaying informational dialogs about the shared personal information.

The *affect-based* category includes the reputation of the third-party that receives the personal information, referral, recommendation and word-of-mouth (Kim et.al, 2008). These affect-based antecedents are all indirect interactions with others, like family and friends, which form feelings and beliefs. This informal interaction with friends and family is also referred to as word-of-mouth (Dichter, 1966). In general people trust their family and friends and therefore they might influence ones risk perception. So when a single sign-on system is recommended by friends and family, it increases trust and therefore decreases the perceived risk (Kim et. al, 2008). People who experience positive affect make more optimistic risk estimates than negative affect does (Johnson & Tversky, 1983). Also media coverage can increase the level of concern for information privacy (Westin, 1990). When there has been a lot of negative messages concerning online privacy, than this information is activated in people's minds. When these messages are very recent, it is easier for people to recall this information from the mind when they find themselves in a situation of disclosing personal information. This way media coverage can increase the perceived risk. Another way risk perception can be influenced by affect is when the third-party is perceived to have a good reputation. This reputation is based on information from a third party. A good reputation will decreases the perceived risk. Therefore these affect antecedents might influence the level of the perceived risk.

The *experience-based* antecedents include familiarity with the involved organization and the previous experiences with, in this case, disclosing personal information (Kim et.al., 2008). Previous personal experiences with online privacy might influence one's information privacy concerns and thereby one's perceived risk (Culnan 1993, Stone & Stone, 1990). When people are able to make a choice more than once, they can get feedback from the previous decisions and learn from it (Hertwig et.al., 2004). Experience is also related with habits, where increasing experience creates the opportunity to reinforce habits (Venkatesh et. al., 2012). With a lot of experience, people create a habit and show routine behavior. Also the outcomes of previous decisions can influence the risk perception (Sitkin & Weingart, 1995). When people have positive experiences with this risk and their privacy has never been violated before, the perceived risk will decrease. When someone's privacy was violated before, this experience might create a higher level of perceived risk that it will happen again. This also works the other way round, it is very likely that more experience with a single sign-on system will decrease the level of the perceived risk, except for negative experiences. So the experience based antecedents are based on how many times people have used a single sign-on system before, and how these experiences are evaluated.

The *personality-oriented* antecedents include a person's dispositional characteristics and habits. First of all a person's general level of concern will influence the risk perception for online privacy risks. As a person's characteristics and habit are quite stable, it is logical to state that people who are generally more concerned about their online privacy, have a higher level of risk perception. Also people who are less concerned about their online privacy will have a lower level of risk perception. When someone is concerned it means that this person worries or feels anxiety about possible negative outcomes (Oxford dictionary, 2015). Some people tend to be more concerned about their

online privacy than others. For example women tend to be more concerned about their online privacy, than men are (O'Neil, 2001). Women do not only tend to perceive a greater severity to the likelihood of negative outcomes, but also to the consequences of the negative outcomes (Garbarino & Strahilevitz, 2004). Another personal characteristic that influences the perceived risk is social criticism. The degree to which someone accepts or rejects social norms, values and practices of society influences the level of concern and thus the perceived risk. It is proposed that people who strongly reject society's values, norms and practices are more likely to be highly concerned about their privacy (Smith et.al., 1996). Personality-oriented antecedents are dependent on a person's characteristics, which are quite stable and therefore are difficult to manipulate, therefore this category is left out of this study.

2.2 What benefits people do perceive when linking new accounts to existing accounts

In a situation where people have to make a decision that involves risks, people make a decision based on the expected value (Kahneman & Tversky, 1979). Most of the time people do things because they gain benefit from it. A benefit is people's perception on the extent to which they will gain an advantage, which can enhance or promote one's well-being (Free dictionary, 2015). People have the possibility to create a new account with only one click by linking it to an existing account, which is referred to as Single Sign-On systems. There are a couple of benefits related to single sign-on systems. First of all, using a single sign-on system saves a lot of time and effort because it is not needed to fill out all the personal information. The information from the single sign-on system (for example Facebook Connect) is automatically shared with the new account. Another example of a benefit is that with linking accounts, people only have to remember one username and one password. This is a benefit because people do have numerous different accounts with different usernames and passwords to remember. Both these benefits come down to convenience, as save a lot of time and effort.

On the other hand it is assumed that these benefits also influence the perceived risk, for example when people have only one password for multiple accounts. When this password is leaked or hacked this gives access to multiple accounts, when people have different passwords for different accounts, this could cause less damage. The possibility of one negative outcome is bigger than the possibility of multiple separate negative outcomes.

2.3 The trade-off between benefits and risks of linking accounts.

In the situation of creating a new account people have the option to fill out their personal information again or by linking it to an existing account (for example Facebook account). There are three risks involved with disclosing personal information (financial, social, and psychological). When internet users do perceive these privacy risks, they do not give away their privacy without realizing that they can gain benefits in return (Culnan, 2000). The benefit for using single sign-on systems is convenience. Rationally seen, people do make a trade-off between the benefits and the risks. This trade-off is referred to as the 'privacy calculus' (Laufer & Wolfe, 1977). When the benefits outweigh the risks, a decision can be made. In some situations the outcomes and the probabilities are easy to determine. In the situation described above, people do not make a choice with a description of possible outcomes or probabilities. People are not able to predict the probability that their personal information will be misused. This means that when they have to decide whether to disclose personal

information or not, they rely on their personal experience, their own observations and word-of-mouth (Hertwig et.al., 2004).

The two antecedent categories (affect and experience) together can create different situations which could result in different risk perceptions that might change the outcome of the final trade-off. This risk perception will together with the perceived benefit lead to a trade-off. This trade-off will decide whether people will engage with using a single sign-on system.

2.4 Theoretical model

Figure 1 shows the theoretical model that is used to explain how previous experiences with a single sign-on system and word-of-mouth influence risk perception, and how time and effort saving influence the benefit perception. The risk perception will together with the benefit perception lead to a trade-off between the risks and benefits. This trade-off leads to the final decision whether to engage in a Single Sign-On system or not.

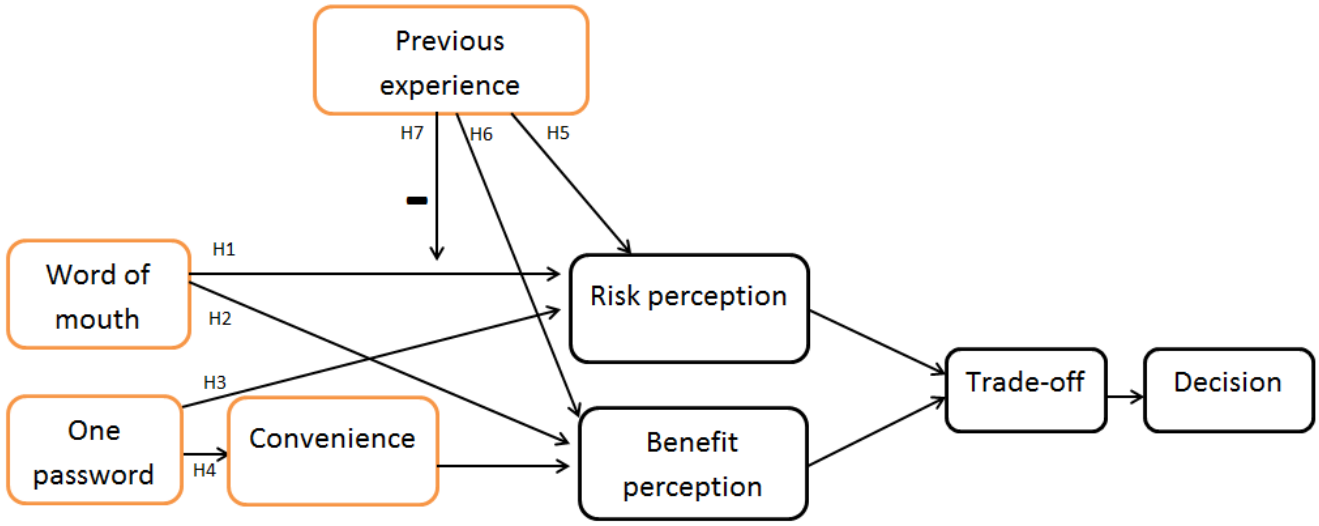


Figure 1 Theoretical model

Previous literature shows that positive affect-based antecedents will decrease the perceived risk, whereas negative affect-based antecedents will increase the perceived risk (Kim et. al., 2008). This means that positive word-of-mouth will decrease the perceived risk, whereas negative word-of-mouth will increase the perceived risk. The same effect applies to benefit perception, where positive word-of-mouth about the single sign-on system will increase the benefit perception and negative word-of-mouth will decrease the benefit perception. This leads to the following hypotheses:

H1. Positive word-of-mouth leads to lower perceived risk than no word-of-mouth.

H2. Positive word-of-mouth leads to higher perceived benefit than no word-of-mouth.

By making use of a single sign-on system, people only need to remember one password instead of multiple passwords. This can influence both the risk perception and convenience. When the one password is leaked or hacked, unwanted people have access to multiple accounts instead of only one account. With multiple passwords, the hack of only one password will only lead to access to one

account.

Having only one password for multiple accounts is easier to remember and therefore more convenient than having multiple passwords. As convenience is assumed to be a benefit in this situation it leads to a higher perceived benefit. This leads to the following hypotheses:

H3. Having one password will lead to a higher perceived risk, than having to remember multiple passwords.

H4. Having one password will lead to more convenience, than having to remember multiple passwords.

Previous experience with using a single sign-on system is can change your perceptions, because this experience will be evaluated in a positive or negative way. Previous experience will influence future choices, through the effect it has on the perceived risk and the perceived benefit. Positive previous experience with a single sign-on system will decrease the perceived risk and negative previous experience with a single sign-on system will increase the perceived risk. On the other hand, previous experiences can also influence the perceived benefit, as positive experiences will increase the perceived benefit and negative experiences will decrease the perceived benefit.

H5. Positive experience with single sign-on systems leads to lower perceived risk than no experience with single sign-on systems.

H6. Positive experience with single sign-on systems leads to higher perceived benefit than no experience with single sign-on systems.

Word-of-mouth and previous experience are both antecedents that influence the risk perception (Kim et. al., 2008). It is assumed that people value their own experience and beliefs higher than information from others. This means that previous experience affects the relation word-of-mouth and risk perception.

H7. The effect of word-of-mouth on risk perception decreases when previous experience increases.

3. Methodology

This study examined the relations between word-of-mouth, having one password and previous experience on people's risk perception and benefit perception.

Experiment

In order to empirically test the hypotheses, an experiment was conducted. This experiment was conducted via an online survey. An online survey was chosen because people who use internet must have heard about some of the online risks. The survey was in Dutch, because the respondents of the convenience sample were Dutch and not everybody understands the questions when in English. There are two manipulated variables: word-of-mouth and having one password with a single sign-on system. Each variable has two possible manipulations, therefore the experiment consisted of 4 different scenarios.

In each of the four scenarios the respondent was faced with the scenario that there exists a new online game that can be played on computer, tablet and smartphone that they would like to play. In order to be able to play this game, they have to create an account so that the scores can be saved. This is the same information for each scenario. The scenarios differ based on the manipulations of word-of-mouth and one password. Each respondent did see one of the four scenarios. The respondents were randomly assigned to one of the scenarios and the scenarios were evenly presented. Based on the scenario the respondents are asked to indicate their risk and benefit perception.

Sample

The sample in this experiment was a convenience sample. The sample consisted of people who use single sign-on systems and people that do not use single sign-on systems. The sample consisted of Dutch respondents because the survey was in Dutch.

Manipulation

Word-of-mouth. The information (word-of-mouth) that others in our environment present us, influences our perceptions. This information is especially important when we have no perception at all about a particular subject. This experiment will test the effect of positive word-of-mouth on the perceived risk and perceived benefit, compared to no word-of-mouth at all. This variable was therefore manipulated in two ways: having word-of-mouth or having no word-of-mouth at all. In the survey the respondents were randomly assigned to one scenario. For this variable 50% of the respondents was assigned to a scenario in which a very close friend says that using a single sign-on system is very easy to use and convenient, compared to creating a new account. The other 50% of the respondents was assigned to a scenario in which this information from a very close friend is left out. For the manipulation a close friend is chosen, because friends are considered to have the most influence (McPhee, 1996).

One password. The single sign-on system allows people to have only one password for multiple accounts, instead having a different password for every single account. This might affect both risk perception and convenience perception. This experiment tested the effect of one password on the perceived convenience and the perceived risk, compared to having multiple passwords. This variable was manipulated in two ways: having only one password for multiple accounts by using a Single Sign-

on system or having multiple passwords by creating a new login for the game. In the first and second scenario the respondents were told that they can login with a single sign-on system, which requires only one password. In the third and fourth scenario the respondents were told that they have to create a new account with a new login and password for this game. For this variable the respondents were randomly assigned, 50% did see the scenario where they can use a single sign-on system and the other 50% did see the scenario where they have to create a complete new account.

Measures

Previous experience. Previous experience with using a single sign-on system influences people's perceptions. This experiment tested the effect of previous experience on risk perception and benefit perception, compared to having no experience with single sign-on systems at all. Also this experiment tested whether previous experience affects the effect of word-of-mouth on risk perception. This construct was measured with two items. The respondents were also asked whether they are familiar with using a single sign-on system. This question is to indicate whether respondents do recognize the single sign-on system phenomenon. Also the respondents had to indicate how much experience they have with using a single sign-on system. This was measured on a seven point Likert-scale where 1 is no experience with single sign-on systems and where 7 is a lot of experience with using a single sign-on system.

Convenience. Using a single sign-on system can save time and effort and therefore brings convenience. The construct convenience was measured with two items. To measure the construct convenience, the respondents had to indicate how convenient they perceive the login system of the game (Kim et.al., 2008) and how much time and effort it saves compared to having no single sign-on system (modified item from Kim et.al., 2008).

Benefit perception. Using a single sign-on system comes with a couple of benefits. The construct benefit perception is measured with two items. Respondents were asked to indicate how much benefit they perceive and how useful the login system is (new modified items).

Risk perception. Disclosing personal information online comes always with risks, because people are not in control of it anymore. The construct risk perception was measured with 7 items. To measure the overall risk perception, the respondents had to indicate on a 7-point Likert scale how their overall perception of risk is for the use of the login system of the game (Kim et.al., 2008). Because online login systems bring three specific risks, these were individually measured. For the financial risk the respondents were asked whether they are afraid for a monetary loss when using the login system for the game (new item based on Biswas & Biswas, 2004). For the social risk the respondents were asked whether they are afraid for (online) bullying and stalking when using the login system for the game (new modified item). For the psychological risk the respondents were asked whether they are afraid that using the login system of the game will negatively affect the respondent's self-esteem (new item based on Mitchel, 1992).

Trade-off. The trade-off construct was measured with one item. In order to measure the trade-off, the question was whether the risks outweigh the benefits or do the benefits outweigh the risks. In order to measure this, the respondents were asked to indicate how much they value the risks compared to how much they value the benefits of using a single sign-on system (new modified item).

Decision. For this experiment the construct *decision* was measured with questions on the intention of using the described login system. Because the scenarios describe a hypothetical online game, it was not possible to measure their decision in a real-life situation. In order to measure the decision whether to engage in using a single sign-on system or a regular login system, the respondents had to indicate how likely they are to use a login system of their scenario on a 7 point Likert scale (Kim et.al., 2004). Also the respondents were asked how likely it is that they would recommend using the login system of their scenario to a friend (Kim et.al., 2004).

At the end of the survey there were three general questions, like gender and age of the respondent and the highest completed education. The questions of the survey including the four scenarios can be found in the appendix.

4. Results

4.1 Data analysis

Demographics

There were 199 respondents that started the survey of which 160 completed the survey (drop-out 20%) and an additional 13 respondents yielded at least some useable data. Of the 160 respondents that completed the survey, 52 (32%) was male and 110 (68%) female. The youngest respondent was 16 and the oldest 77, half of the respondents was younger than 24 and the average age was 24. Regarding the highest finished educational level, 45% of the respondents had finished a WO (bachelor and/or master) study, 22% finished an HBO study, 12% finished a MBO study, and 21% has VMBO, HAVO or VWO as highest finished educational level. This sample is not representative for the whole Dutch population, because the average level of education of the sample is much higher than in the Dutch population (only 33.6% of the population has finished a HBO or WO study) (Eurostat, 2014). This sample contains only one third male and two third female, while the gender distribution for the Dutch population is rather even with slightly more women (CBS, 2014).

Dataset

The construct *decision* is measured with two items that are highly correlated (Pearson: 0.74), also the Cronbach's alpha 0.849 > 0.7 shows reliability. Therefore these items are averaged into the variable *Decision.*

The construct *risk perception* is measured with seven items. As risk perception was operationalized as general, financial, psychological and social risk an explanatory factor analysis was carried out to see whether these items all measure one and the same construct. The principal component analysis with Oblimin rotation implied two components with an eigenvalue > 1. Also the scree plot indicated 2 components. The correlation between these two components was 0.17 which is rather low, which supports the decision for two components. One component that existed of the general risk perception items and the financial risk perception item, this component will be called the general-economic-risk. The other component existed of the psychological risk item and the social risk item, this component is called the psycho-socio-risk. The Cronbach's alpha for the general-economic-risk is 0,865 which is >0.7 and therefore acceptable. The Cronbach's alpha for the psycho-socio-risk is 0.754

which is >0.7 and therefore also acceptable. The averages of the items of each of the two components are added to the database as two new variables.

The constructs benefit and convenience are measured with four items. These items look a lot like each other, because convenience is the main benefit of a single sign-on system. Because of this, the items of these two separate constructs were put into a factor analysis in order to check whether they can be distinguished. The Principal component analysis showed one eigenvalue >1 and also a scree plot which indicated one component. Therefore the four items that measure convenience and benefit perception were averaged into a new variable: *benefit*.

The trade-off construct exists from only one item and therefore it is not needed to create a new item and it is not possible to check the reliability.

4.2 Test hypotheses

A regression shows that the trade-off between risks and benefits influences the intention to adapt a single sign-on system with correction for *gender* ($F(2, 159) = 22.12$, $p<0.01$, $R^2=0.22$). With *the trade-off* scoring higher importance of risk resulting in lower *adoption intention* (B= -0.45). No effect was found for *gender* ($t(159) = -0.59$, $p=0.55$, B=-0.14).

A multiple regression with *benefit*, *psycho-socio risk*, *general-economic risk* predicting the trade-off with correction for gender was significant ($F(4, 157) = 11.13$, $p<0.01$, $R^2= 0.22$) with higher *general-economic risk* showing higher risk in *trade-off* ($t(157) = 4.86$, $p<0.01$, B=0.0.40), no effect of *psycho-socio risk* ($t(157) = 0.29$, $p=0.77$, B=0.03), and increased *benefit* showed a lower risk in *trade-off* ($t(157) = -2.81$, $p<0.01$, B=-0.26). No effect was found for *gender* ($t(157) = 1.56$, $p=0.12$, B=0.38).

In order to test H1, H3, H5 and H7 a factorial ANOVA with *word-of-mouth, one password* and *experience* (and all two-way and three-way interactions) on *psycho-socio risk* corrected for gender was conducted ($F(8, 153) = 2.61$, $p<0.05$). No main effects of *word-of-mouth* ($F(1, 154) = 0.23$, $p=0.63$) or *one password* ($F(1, 153) = 0.13$, $p=0.72$) on *psycho-socio risk* were found. There was a main effect of *experience* ($F(1, 153) = 7.47$, $p<0.01$, B=-0.87) with less *previous experience* showing higher *psycho-socio risk*. Neither the interaction of *word-of-mouth* with *one password* ($F(1, 153) = 0.58$, $p=0.45$), nor *word-of-mouth* with *experience* ($F(1, 153) = 1.58$, $p=0.21$), nor *one password* with *experience* ($F(1, 153) = 1.00$, $p=0.32$), nor the three-way interaction ($F(1, 153) = 0.18$, $p=0.67$) were significant. Hence for *psycho-socio risk* only support for H5 was found, where a lower level of *previous experience* showed a higher *psycho-socio risk*. A main effect was found for *gender* ($F(1, 153) = 5.68$, $p<0.01$, B=-0.44), where females perceive higher *psycho-socio risk* than males.

Also a factorial ANOVA with *word-of-mouth, one password* and *experience* (and all two-way and three-way interactions) on *general-economic risk* with correction for *gender* was conducted ($F(8, 153) = 4.34$, $p<0.01$). No main effect of *word-of-mouth* on *general-economic risk* ($F(1, 153) = 1.82$, $p=0.18$) and *experience* ($F(1, 153) = 2.52$, $p=0.11$) was found. A main effect was found for *one password* ($F(1, 153) = 23.31$, $p<0.01$, B=-1.19) on *general-economic risk*, with *one password* showing higher *general-economic risk*. Neither the interaction of *one password* and *experience* ($F(1, 153) = 1.68$, $p=0.20$), nor *word-of-mouth* and *one password* ($F(1, 153) = 0.07$, $p=0.79$), nor *word-of-mouth* and *experience* ($F(1, 153) = 0.22$, $p=0.64$) were significant. Hence for *general-economic risk* support for H3 was found. No effect was found for *gender* on *general-economic risk*.

In order to test H2, H4 and H6 a factorial ANOVA with *word-of-mouth, one password* and *experience* (and all two-way and three-way interactions) on *benefit* was conducted with correction for gender ($F(8, 153) = 1.68$, $p=0.11$). No main effects of *word-of-mouth* ($F(1, 153) = 2.22$, $p=0.14$) or *experience* ($F(1, 153) = 0.02$, $p=0.89$) on *benefit* were found. A main effect was found for *one password* ($F(1, 153) = 3.90$, $p<0.05$, $B=-0.63$), with *one password* showing higher *benefit*. Neither the interaction of *one password* and *experience* ($F(1, 153) = 0.01$, $p=0.93$), nor *word-of-mouth* and *one password* ($F(1, 153) = 0.23$, $p=0.63$), nor *word-of-mouth* and *experience* ($F(1, 153) = 2.02$, $p=0.16$), nor the three way interaction ($F(1, 153) = 0.37$, $p=0.54$). Hence for *benefit* support for H4 was found. Also a main effect for gender on *benefit* ($F(1, 153) = 4.14$, $p<0.05$, $B=0.42$) was found, where males perceive higher *benefit*.

Table 1 shows the means per construct for each scenario. The means indicate the direction and strength of each construct. The table shows relatively low means for the *psycho-socio risk* while relatively high means for *general-economic risks* and *benefit* and *trade-off*. The means for the *decision* to adapt a single sign-on system are not relatively high or low.

Table 1. Means per construct, per scenario (standard deviations between brackets).

	General-economic risk	**Psycho-socio risk**	**Benefit**	**Trade-off**	**Decision**
Word-of-mouth & one password (scenario 1)(N=44)	4.83 (1.31)	1.82 (1.03)	4.27 (1.07)	4.86 (1.53)	3.11 (1.63)
No word-of-mouth & one password (scenario 2)(N=45)	4.65 (1.28)	1.97 (0.94)	4.32 (1.01)	4.53 (1.68)	3.50 (1.45)
Word-of-mouth & multiple password (scenario 3)(N=37)	3.90 (1.19)	1.78 (1.08)	3.83 (1.30)	4.31 (1.45)	3.85 (1.53)
No word-of-mouth & multiple password (scenario 4)(N=40)	3.67 (1.40)	2.15 (1.30)	3.93 (1.28)	4.26 (1.52)	3.73 (1.47)

A multiple hierarchical regression was conducted in order to check whether there are remaining direct effects of *psycho-socio risk*, *general-economic risk* and *benefit* on *decision* after *trade-off* is included with correction for gender (F change $(3, 156) = 40.33$, $p<0.01$, R^2 change$= 0.34$). Main effects were found for *general-economic risk* ($t(156) = -6.16$, $p<0.01$, $B=-0.40$) and *benefit* ($t(156) = 9.11$, $p<0.01$, $B=0.64$). With *general-economic risk* showing lower adaption intention and with higher *benefit perception* showing higher adaption intention. No main effect was found for *psycho-socio risk* ($t(156) = 1.48$, $p=0.14$).

5. Conclusion & discussion

5.1 Conclusions and implications

The results from the data analyses lead to the revised model in figure 2.

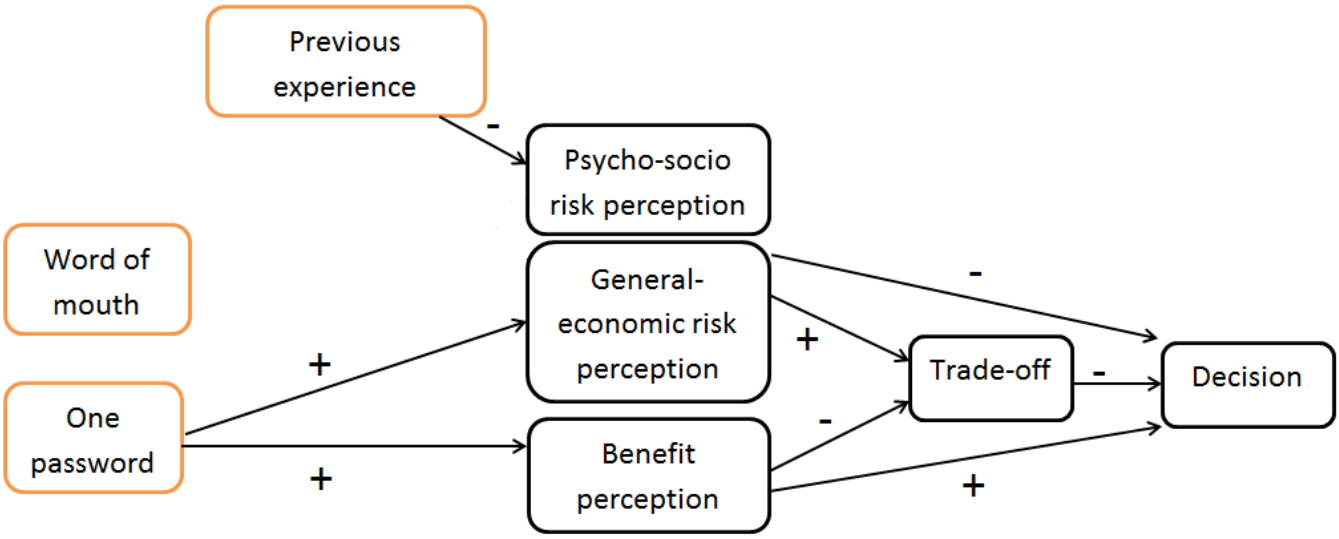


Figure 2 Revised model

The revised model (figure 2) shows some interesting findings. The most striking finding is that the main benefit of single sign-on systems, having one password, has a positive effect on the benefit perception and the general-economic risk perception. This means that having one password and thus using a single sign-on system on the one hand increases the perceived benefit, while on the other hand it also increases the perceived general-economic risk. Single Sign-on systems require only one password, which can result in ambivalence towards the general-economic risks and benefits. This is interesting because most constructs increase the benefit or the risk, while it decreases the other. People see the benefit and the convenience of having to remember only one password, but they also feel the risk that their password might end up in unwanted hands it could cause financial damage. Because of these contradicting feelings a trade-off is needed to make a final decision.

Single sign-on systems could influence the general-economic risk perception by decreasing the risk perception or improving the benefit perception. The general-economic risk perception could decrease when people feel that their personal information is protected better and handled with a better security system. Therefore it is important that single sign-on system communicate about the security of their personal information. Another option is to make it more difficult for hackers to hack passwords, for example by demanding more complex passwords where people have to use at least one capital, two numbers and one symbol (Nelson & Vu, 2010; Vu et.al. 2003). This option would on the other hand make having one password less convenient and therefore decrease the benefit perception. Another option to decrease the general-economic risk perception is to ask users to change their password every once in a while (Vu et.al., 2007). This could also decrease the benefit perception, this makes it harder to remember the one password if you have to change it every now and then. Another option to increase the security of the password and thereby decrease the general-economic risk perception is with a biometric password (Prabhakar, 2003). This is for example logging in by using a finger print or iris scan. Previous research shows, that even though the limited level of

practical experience, a relatively high acceptance for biometric passwords already exists (Furnell & Evangelatos, 2007). People perceive that this system is very hard to cheat on, and most people perceive leaving a fingerprint as most reliable compared to other biometric passwords. As this is quite a new phenomenon and people lack the experience with these systems, it would be interesting for further research to investigate how previous experience could enhance the level of acceptance of biometric passwords.

It can also be concluded that previous experience with single sign-on systems decreases the psycho-socio risk. So when people are familiar with single sign-on systems they perceive the possibility that using a single sign-on system will harm their social status, as very low. The psycho-socio risk seems to have no effect on the trade-off or adaption of single sign-on systems. Still this is an interesting and important finding because previous experience undermines trust in Facebook. When people do not trust Facebook, and maybe do not have a Facebook account at all, they are not likely or able to use FacebookConnect as a single sign-on system. It could be that people are bullied on social media before and therefore perceive psycho-socio risks with using single sign-on systems. Previous experience could create trust in the system and in the actor (for example Facebook) and understanding in the system/service. Trust in the system/service can influence the decision to engage in using single sign-on systems (Gefen et.al., 2003). When people trust the system or actor because of positive previous experience this could decrease the risk perception (Sitkin & Weingart, 1995). Although trust is not measured in this study it could indirectly influence the decision to adapt single sign-on systems, by decreasing the psycho-socio risk perception. On the other hand risk perception might influence people's trust. For further research it could be interesting how trust interacts in the model.

It is interesting to see that there is an actual difference between general-economic risks and psychological-social risks. People feel the possibility and uncertainty of a financial loss and stalking and bullying as two separate risks. These risks are measured as two different risks, which should be kept an eye on in further research. The general-economic risk is something that is inevitable in situations where money is involved, but the psycho-socio risk could be decreased by separating the single sign-on systems from social media. In this study FacebookConnect and Twitter are used as examples of single sign-on systems and might be the most well-known single sign-on systems, but this could mean that people perceive higher psycho-socio risks compared to single sign-on systems that are not linked to social media. For further research it could be interesting to see how strong these risk perceptions are for a new made-up single-sign on system that does not interact with social media.

The general-economic risk perception and the benefit perception both influence the trade-off, where a higher benefit perception decreases the risk in trade-off while the general-economic risk perception increases the risk in trade-off. This means that when people do not perceive any or low benefit from using a single sign-on system, but do perceive more or only general or economic risks with using single sign-on systems, the risk in trade-off results in a lower adaption of single sign-on systems. Also when people perceive more benefits or benefits only, with no or lower general or economic risks, the lower risk in trade-off will result in a higher adaption of single sign-on systems.

There were some effects found for gender in this revised model. Women do perceive higher psycho-socio risks than men do and men do perceive higher benefit. It seems that women are more

concerned about risks, while men are more sensitive to the benefits in this situation. It could be interesting to find out where these differences come from.

5.2 Limitations

Something interesting that was found is that *word-of-mouth* does seem to have no effect on the *general-economic risk, psycho-socio risk* and *benefit perception.* The *word-of-mouth* construct was manipulated in the scenarios, by stating that the respondent's friends play the online game and are very enthusiastic about it and that they use Facebook to login. It is possible that this construct is manipulated wrong and therefore does not give the same results that were found in literature. Instead of manipulating this construct it is also possible to measure this item, by for example asking whether their friends are using single sign-on systems. For further research it would be interesting to study whether *word-of-mouth* does influence the risk perception and benefit perception for single sign-on systems.

In the revised model it is shown that *general-economic risk perception* and *benefit perception* do have direct effects on the *decision* to adapt a single sign-on system. The theory shows that *general-economic risk perception* and *benefit perception* come together in a trade-off where people weigh the benefits and risk in order to make a decision. This could mean that the construct *trade-off* is not measured correctly. It was measured with only one item where the respondents had to indicate what they value more when deciding to adapt a single sign-on system, the benefits or the risk that come along with it. It could be that one item is not enough for this construct. On the other hand it might be that the item that is used does not measure what it is intended to measure. It is also possible that people do not make a trade-off between the risks and benefits, or that they are not consciously aware of this trade-off. For further research it would be advised to do further research in the role of this trade-off for the decision. It could also be explained by the fact that people are often nudged to use single sign-on system, because the buttons for single sign-on systems are made more visible than the option to create a new account with your e-mail address. This way the benefit of creating a new account with only one click, is more present and immediate than the risks that come to mind at the moment of trade-off and decision.

In the theoretical model *convenience* was distinguished from *benefit,* but after a Principal component analysis the four items seem to measure them as one construct. For further research it could help to precisely define both constructs, what should make it easier to measure them as two separate constructs.

Another limitation of this study is that the sample is not representative for all Dutch people. This can be ascribed to the fact that this study used a convenience sample. The educational level of the sample is relatively high and the age of the respondents is relatively low. For future research it is recommended to have an equal distribution in the level of education and age, so that it becomes representative for all Dutch people. Another option is to compare at the expected values of age and education with the observed values.

There were a couple of respondents that said they did not use single sign-on systems, but when giving a concrete example of a FacebookConnect implementation, they recognized the system. It could be that the introduction of single sign-on systems was not clear enough for everyone to understand. This could have biased the results, especially the questions whether people are familiar

with single sign-on systems and which of them they use. For further research it is advised to insert a picture of a FacebookConnect button for example, because this is more recognizable for respondents.

5.3 Final conclusion

Previous positive and negative experiences with single sign-on systems are of significant importance for people's psycho-socio risk perception. The most interesting finding in the model is that having one password for multiple accounts leads to an increased benefit perception and increased general-economic risk perception at the same time. This means people feel ambivalent towards single sign-on systems which results in a trade-off where an increased general-economic risk perception increases the risk in trade-off and an increasing benefit perception decreases the risk in trade-off. Finally, the higher the risk in trade-off, the lower the intention to decide to adapt single sign-on systems.

References

Acquisti, A., & Gross, R. (2006, January). Imagined communities: Awareness, information sharing, and privacy on the Facebook. In Privacy enhancing technologies (pp. 36-58). Springer Berlin Heidelberg.

Anderson, E., & Weitz, B. (1989). *Determinants of continuity in conventional industrial channel dyads*. Marketing science, 8(4), 310-323.

Bart, Y., Shankar, V., Sultan, F., & Urban, G. L. (2005). *Are the drivers and role of online trust the same for all web sites and consumers? A large-scale exploratory empirical study*. Journal of marketing, 69(4), 133-152.

Bauer, L., Bravo-Lillo, C., Fragkaki, E., & Melicher, W. (2013, November). *A comparison of users' perceptions of and willingness to use Google, Facebook, and Google+ single-sign-on functionality*. In Proceedings of the 2013 ACM workshop on Digital identity management (pp. 25-36). ACM.

Besmer, A., & Lipford, H. R. (2010, May). Users'(mis) conceptions of social applications. In Proceedings of Graphics Interface 2010 (pp. 63-70). Canadian Information Processing Society.

Biswas, D., & Biswas, A. (2004). *The diagnostic role of signals in the context of perceived risks in online shopping: do signals matter more on the web*?. Journal of Interactive Marketing, 18(3), 30-45.

Chen, H. T., & Kim, Y. (2013). *Problematic Use of Social Network Sites: The Interactive Relationship Between Gratifications Sought and Privacy Concerns*. Cyberpsychology, Behavior, and Social Networking, 16(11), 806-812.

Corbitt, B. J., Thanasankit, T., & Yi, H. (2003). *Trust and e-commerce: a study of consumer perceptions*. Electronic commerce research and applications, 2(3), 203-215.

Crespo, A. H., del Bosque, I. R., & de los Salmones Sanchez, M. G. (2009). *The influence of perceived risk on Internet shopping behavior: a multidimensional perspective.* Journal of Risk Research, 12(2), 259-277.

Culnan, M. J. (1993). " *How Did They Get My Name?": An Exploratory Investigation of Consumer Attitudes toward Secondary Information Use*. Mis quarterly, 341-363.

Culnan, M. J. (2000). *Protecting privacy online: Is self-regulation working?*. Journal of Public Policy & Marketing, 19(1), 20-26.

Dichter, E. (1966). *How word-of-mouth advertising works*. Harvard business review, 44(6), 147-160.

Dwyer, C., Hiltz, S., & Passerini, K. (2007). *Trust and privacy concern within social networking sites: A comparison of Facebook and MySpace.* AMCIS 2007 Proceedings, 339.

Egelman, S. (2013, April). *My profile is my password, verify me! : the privacy/convenience tradeoff of facebook connect.* In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (pp. 2369-2378). ACM.

Evans, J. S. B. (2003). *In two minds: dual-process accounts of reasoning*. Trends in cognitive sciences, 7(10), 454-459.

Forsythe, S. M., & Shi, B. (2003). *Consumer patronage and risk perceptions in Internet shopping.* Journal of Business Research, 56(11), 867-875.

Furnell, S., & Evangelatos, K. (2007). *Public awareness and perceptions of biometrics*. Computer Fraud & Security, 2007(1), 8-13.

Gambetta, D. (1988), (Ed.), *Trust: Making and Breaking Cooperative Relations*, Basil Blackwell, Oxford pp. 94–107

Garbarino, E., & Strahilevitz, M. (2004). *Gender differences in the perceived risk of buying online and the effects of receiving a site recommendation*. Journal of Business Research, 57(7), 768-775.

Gefen, D., Karahanna, E., & Straub, D. W. (2003). *Inexperience and experience with online stores: The importance of TAM and trust.* Engineering Management, IEEE Transactions on, 50(3), 307-321.

Govani, T., & Pashley, H. (2005). *Student awareness of the privacy implications when using Facebook.* unpublished paper presented at the "Privacy Poster Fair" at the Carnegie Mellon University School of Library and Information Science, 9.

Hertwig, R., Barron, G., Weber, E. U., & Erev, I. (2004). *Decisions from experience and the effect of rare events in risky choice*. Psychological Science, 15(8), 534-539.

Jacoby, J., & Kaplan, L. B. (1972). *The components of perceived risk*. Advances in consumer research, 3(3), 382-383.

Johnson, E. J., & Tversky, A. (1983). *Affect, generalization, and the perception of risk*. Journal of personality and social psychology, 45(1), 20.

Kahneman, D., & Tversky, A. (1979). *Prospect theory: An analysis of decision under risk*. Econometrica: Journal of the Econometric Society, 263-291.

Khaneman, D. (2003). *A perspective on judgement and choice*. American Psychologist, 58, 697-720.

Kim, D. J., Ferrin, D. L., & Rao, H. R. (2008). *A trust-based consumer decision-making model in electronic commerce: The role of trust, perceived risk, and their antecedents*. Decision support systems, 44(2), 544-564.

Krasnova, H., Günther, O., Spiekermann, S., & Koroleva, K. (2009). Privacy concerns and identity in online social networks. Identity in the Information Society, 2(1), 39-63

Kumar, N., Scheer, L. K., & Steenkamp, J. B. E. (1995). *The effects of perceived interdependence on dealer attitudes*. Journal of marketing research, 348-356.

Laufer, R. S., & Wolfe, M. (1977). *Privacy as a concept and a social issue: A multidimensional developmental theory*. Journal of Social Issues, 33(3), 22-42.

Eun Lee, J., & Stoel, L. (2014). *High versus low online price discounts: effects on customers' perception of risks*. Journal of Product & Brand Management, 23(6), 401-412.

Mayer, R. C., Davis, J. H., & Schoorman, F. D. (1995). *An integrative model of organizational trust*. Academy of management review, 20(3), 709-734.

McPhee, J. H. (1996). *Influence strategies in young adolescent dyads*. Dissertation Abstracts International, 57(02), 1468B.

Mitchell, V.-W., (1992). *Understanding consumers' behavior: can perceived risk theory help?* Management Decision, 30 (2), 26–31

Nelson, D., & Vu, K. P. L. (2010). *Effectiveness of image-based mnemonic techniques for enhancing the memorability and security of user-generated passwords.* Computers in Human Behavior, 26(4), 705-715.

Newcom Research & consultancy, 2014, *Nationale social media onderzoek 2014. Januari 2014. The Netherlands.*

O'Neil, D. (2001). *Analysis of Internet users' level of online privacy concerns*. Social Science Computer Review, 19(1), 17-31.

Prabhakar, S., Pankanti, S., & Jain, A. K. (2003). *Biometric recognition: Security and privacy concerns.* IEEE Security & Privacy, (2), 33-42.

Ridings, C. M., Gefen, D., & Arinze, B. (2002). *Some antecedents and effects of trust in virtual communities*. The Journal of Strategic Information Systems, 11(3), 271-295.

Sitkin, S. B., & Weingart, L. R. (1995). *Determinants of risky decision-making behavior: A test of the mediating role of risk perceptions and propensity*. Academy of management Journal, 38(6), 1573-1592.

Smith, H. J., Milberg, S. J., & Burke, S. J. (1996). *Information privacy: measuring individuals' concerns about organizational practices.* MIS quarterly, 167-196.

Statista, 2014*, Most popular social media websites in the United States in September 2014, based on share of visits.* Statista, the statistics portal. September 2014.

Stone, E. F., & Stone, D. L. (1990). *Privacy in organizations: Theoretical issues, research findings, and protection mechanisms.* Research in personnel and human resources management, 8(3), 349-411.

Tversky, A., & Fox, C. R. (1995). *Weighing risk and uncertainty*. Psychological review, 102(2), 269.

Venkatesh, V., Thong, J. Y., & Xu, X. (2012). *Consumer acceptance and use of information technology: extending the unified theory of acceptance and use of technology*. MIS quarterly, 36(1), 157-178.

Vu, K. P. L., Bhargav, A., & Proctor, R. W. (2003, October). *Imposing password restrictions for multiple accounts: Impact on generation and recall of passwords*. In Proceedings of the human factors and ergonomics society annual meeting (Vol. 47, No. 11, pp. 1331-1335). SAGE Publications.

Vu, K. P. L., Proctor, R. W., Bhargav-Spantzel, A., Tai, B. L. B., Cook, J., & Schultz, E. E. (2007). *Improving password security and memorability to protect personal and organizational information*. International Journal of Human-Computer Studies, 65(8), 744-757.

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

Young, A. L., & Quan-Haase, A. (2009, June). *Information revelation and internet privacy concerns on social network sites: a case study of facebook*. In Proceedings of the fourth international conference on Communities and technologies (pp. 265-274). ACM.

Dictionaries:
Oxford dictionaries, 2015, www.oxforddictionaries.com

The Free Dictionary, 2015, www.thefreedictionary.com/risk.

Appendix

Beste deelnemer

Fijn dat u mee wilt doen aan dit onderzoek. Het onderzoek is uitsluitend bedoeld voor academische doeleinden en er zijn geen commerciële bedrijven bij betrokken.

Het invullen van de vragenlijst duurt ongeveer 10 minuten. Deelname is geheel anoniem.

U kunt op elk moment tijdens het onderzoek beslissen om te stoppen met invullen. Het afronden van het onderzoek wordt beschouwd als toestemming voor deelname in dit onderzoek. Let op bij het invullen, want er is geen mogelijkheid om terug te keren naar een voorafgaande vraag.

U ziet zometeen een tekst die u goed dient door te lezen. Op basis van deze tekst krijgt u een aantal vragen en er is geen mogelijkheid om terug te gaan naar deze tekst.

Scenario 1
Er is een nieuw online spel dat je graag wilt spelen op je computer, telefoon of tablet. Hiervoor moet je een account aanmaken, zodat je scores kunnen worden opgeslagen. Je maakt hiervoor gebruik van een Single Sign-on systeem (OpenID / Facebook Connect). Dit betekent dat je persoonlijke gegevens en financiële gegevens door het Single Sign-on systeem worden overgedragen aan de organisatie van het spel en dus hoef je deze niet opnieuw in te vullen. Om in te kunnen loggen gebruik je één en hetzelfde wachtwoord als voor andere websites en apps waarmee je inlogt via je Single Sign-on systeem.

Je vrienden hebben je verteld over dit te gekke spel en spelen dit via Facebook, omdat het heel gemakkelijk werkt en je gemakkelijk de scores van je vrienden bij kunt houden.

Scenario 2
Er is een nieuw online spel dat je graag wilt spelen op je computer, telefoon of tablet. Hiervoor moet je een account aanmaken, zodat je scores kunnen worden opgeslagen. Je maakt hiervoor gebruik van een Single Sign-on systeem (OpenID / Facebook Connect). Dit betekent dat je persoonlijke gegevens en financiële gegevens door het Single Sign-on systeem worden overgedragen aan de organisatie van het spel en dus hoef je deze niet opnieuw in te vullen. Om in te kunnen loggen gebruik je één en hetzelfde wachtwoord als voor andere websites en apps waarmee je inlogt via je Single Sign-on systeem.

Scenario 3
Er is een nieuw online spel dat je graag wilt spelen op je computer, telefoon of tablet. Hiervoor moet je een account aanmaken, zodat je scores kunnen worden opgeslagen. Om in te kunnen loggen maak je een nieuw account aan met een nieuwe inlognaam en wachtwoord, speciaal voor dit spel.

Je vrienden hebben je verteld over dit te gekke spel en spelen dit via Facebook, omdat het heel gemakkelijk werkt en je gemakkelijk de scores van je vrienden bij kunt houden.

Scenario 4
Er is een nieuw online spel dat je graag wilt spelen op je computer, telefoon of tablet. Hiervoor moet je een account aanmaken, zodat je scores kunnen worden opgeslagen. Om in te kunnen loggen maak je een nieuw account aan met een nieuwe inlognaam en wachtwoord, speciaal voor dit spel.

Geef aan in hoeverre u het eens bent met de volgende stellingen:

	1 mee oneens	2	3	4	5	6	7 mee eens
Het inlogsysteem van dit spel is erg gebruiksvriendelijk	○	○	○	○	○	○	○
Het inlogsysteem bespaart mij tijd	○	○	○	○	○	○	○
Ik zie alleen maar voordelen aan het inlogsysteem	○	○	○	○	○	○	○
Ik vind het inlogsysteem erg handig	○	○	○	○	○	○	○

Geef aan in hoeverre u het eens bent met de volgende stellingen:

	1 mee oneens	2	3	4	5	6	7 mee eens
Ik zie het als risicovol om op deze manier in te loggen voor het spel	○	○	○	○	○	○	○
Ik maak me zorgen over de veiligheid van mijn persoonlijke gegevens	○	○	○	○	○	○	○
Ik zie alleen maar risico's verbonden aan deze manier van inloggen bij het spel	○	○	○	○	○	○	○
Ik ben bang voor financiële schade wanneer ik op deze manier inlog bij dit spel	○	○	○	○	○	○	○
Ik ben bang voor online pesten en stalken wanneer ik op deze manier inlog bij dit spel	○	○	○	○	○	○	○
Ik ben bang dat het gebruik van dit inlogsysteem bij het spel mijn zelfvertrouwen kan schaden	○	○	○	○	○	○	○
Ik ben bang dat mijn gegevens zonder mijn toestemming in handen van derden zullen vallen	○	○	○	○	○	○	○

Geef aan in hoeverre u het eens bent met de volgende stellingen:

	1 mee oneens	2	3	4	5	6	7 mee eens
Ik zou mijn vrienden aanraden om op deze manier een account te maken en in te loggen voor dit spel	○	○	○	○	○	○	○
Ik zou voor het eerdergenoemde online spel inloggen zoals beschreven in de tekst aan het begin van deze survey	○	○	○	○	○	○	○

Bent u bekend met het gebruik van Single Sign-on systemen zoals FacebookConnect, Twitter en OpenID? Dit zijn inlog-systemen waarbij u met 1 gebruikersnaam en 1 wachtwoord in kunt loggen op allerlei apps en websites, u hoeft dus geen nieuw account aan te maken.

ja	nee
○	○

Welke van de volgende Single Sign-on systemen zijn u bekend?

	ja	nee
FacebookConnect	○	○
Twitter	○	○
OpenID	○	○

Hoe vaak kiest u ervoor om in te loggen met Single Sign-on systemen zoals OpenID en FacebookConnect om een nieuw account aan te maken (voor bv apps en sites)? Geef aan op een schaal van 1 tot 7, waarbij 1 is nooit en 7 is altijd

1, Ik gebruik nooit een Single Sign-on systeem	2	3	4	5	6	7, Ik gebruik altijd een Single Sign-on systeem waar mogelijk
○	○	○	○	○	○	○

Welk Single Sign-on systeem gebruikt u het meest?

- ○ FacebookConnect
- ○ Twitter
- ○ OpenID
- ○ Geen
- ○ Anders, namelijk:

Geef aan wat u belangrijker vindt bij de keuze voor het gebruik van een Single Sign-on systeem. Wegen de voordelen zwaarder voor u of wegen de risico's zwaarder?

1 Voordelen	2	3	4 Neutraal / even zwaar	5	6	7 risico's
○	○	○	○	○	○	○

Geef aan in hoeverre u er vertrouwen in hebt dat uw persoonlijke gegevens goed beschermd worden bij het gebruik van een Single Sign-on systeem.

1, geen vertrouwen	2	3	4	5	6	7, vol vertrouwe
○	○	○	○	○	○	○

Geef aan in hoeverre u het eens bent met de volgende stellingen:

	1, mee oneens	2	3	4	5	6	7, mee eens
Ik heb vertrouwen in FacebookConnect als Single Sign-on systeem	○	○	○	○	○	○	○
Ik heb vertrouwen in Twitter als aanbieder van een Single Sign-on systeem	○	○	○	○	○	○	○
Ik heb vertrouwen in OpenID als aanbieder van een Single Sign-on systeem	○	○	○	○	○	○	○

Wat is uw geslacht?

- ○ Man
- ○ Vrouw

Wat is uw leeftijd?

Wat is uw hoogst **afgeronde** opleiding?

- ○ Voorgezet onderwijs (VMBO/HAVO/VWO)
- ○ MBO
- ○ HBO
- ○ WO (Bachelor en/of Master)

Aan Wageningen Universiteit worden vaker studies verricht waarvoor wij op zoek zijn naar deelnemers. Mogen wij u hiervoor af en toe (maximaal 1 keer per maand) benaderen per e-mail?

Zo ja, schrijf hieronder uw e-mailadres (niet nodig als u dit al eerder heeft aangegeven):

Klaar!
Heeft u nog opmerkingen over deze vragenlijst dan kunt u die hieronder kwijt. Hartelijk dank voor uw deelname aan dit onderzoek.