European Commission

JRC TECHNICAL REPORTS

The Effect of Warning Messages on Secure Behaviour Online

Results from a lab experiment

Nuria Rodríguez-Priego
René van Bavel

2016

EUR 28154 EN

Contact information
Address: Edificio Expo. c/Inca Garcilaso, 3. 41092 Seville (Spain)
E-mail: b06-sec@jrc.ec.europa.eu
Tel.: +34 954488318

JRC Science Hub
https://ec.europa.eu/jrc

JRC103188

EUR 28154 EN

PDF ISBN 978-92-79-62758-3 ISSN 1831-9424 doi:10.2791/597150

Luxembourg: Publications Office of the European Union, 2016

How to cite: Rodríguez-Priego, N. & van Bavel, R. (2016). The Effect of Warning Messages on Secure Behaviour Online: Results from a lab experiment. *JRC Technical Reports.* EUR 28154 EN; doi:10.2791/597150

Table of contents

Acknowledgements

This technical report presents the results of the first experiment conducted as part of the project *Behavioural Insights on Cybersecurity*. The authors are grateful to Ioannis Maghiros for his support as Head of Unit (JRC.B4).

The study was conducted as a lab experiment with the advice of Jose Vila, head of the experimental economics lab LINEEX (ERI-CES – University of Valencia) and Rebeca Parra Orenga, technical manager and software designer. The authors gratefully acknowledge valuable discussions with them and with Professor Pam Briggs, from the University of Northumbria, who participated as external expert.

Abstract

Background

Increasing safety and security online can help boost the opportunities for people and businesses to trade, innovate and interact in digital markets. The level of online security is affected by technical factors, natural events and human behaviour. This study contributes to policy initiatives aimed at getting consumers to increase their online security. It tests several warning messages, based on behavioural insights, which could persuade consumers to behave more securely while online, thus diminishing their chances of suffering a cyber-attack.

Methods

A lab experiment was conducted in Spain (n=600). Participants had to make some online shopping decisions, and were assigned a quantity of money. An additional variable incentive depended on how secure their behaviour was during the purchasing process. Five security behaviours were observed: choosing a safe connection, providing less information during the sign-up process, choosing a strong password, choosing a trusted vendor, and logging-out. Each decision could increase their chances of suffering a cyber-attack at the end of the experiment and losing part of their variable incentive. Other factors that could affect secure behaviour were measured through a pre-purchase and a post-purchase questionnaire.

Findings

Results show that long security messages and messages accompanied by a male anthropomorphic character led consumers to disclose less personal information when signing up to an e-commerce website. A loss-framed message made subjects more likely to choose a trusted vendor and to log out of a website after completing a purchase. It also made them behave more securely when security behaviour is treated as a composite indicator built on three behavioural measures (using trusted vendors, using secure passwords and logging out). None of the treatments was effective in making subjects choose a safe connection, or a stronger password.

Conclusions

The design of security messages has an effect on security behaviour. The policy implications are that security awareness messages should be designed based on behavioural insights and be piloted before implementation. The lack of effect of the security messages on choosing a stronger password should be further examined. This result may be related to consumers lacking information on what a strong password is, or lacking knowledge that could help them to relate stronger passwords with more secure behaviour online.

1. Introduction and policy context

According to *Europe's Digital Progress Report*[1], the number of European citizens ordering goods and services online increased by 13 percentage points between 2010 and 2015, to 53 %. E-commerce is higher among younger and higher educated people, as with many other online activities. However, there are still some concerns about the lack of perceived security of online payments that prevents consumers from using the Internet for e-commerce (27% of respondents), trust concerns about receiving or returning goods, complaint / redress concerns (19% of respondents), and lack of the necessary skills (13% of respondents).

Online security is influenced by natural events, technical failures and malicious threats, but human mistakes also play an important role. People's online behaviour can become repetitive and monotonous, leading them to pay less attention and to attribute less importance to the decision-making process. People also behave unsafely online because they lack knowledge about the consequences of their online behaviour; because they perceive the risks as low; or because they do not follow the recommendations and advice on safety given to them. Users' final actions will be influenced by their own awareness of security risks and their understanding of these, realistic self-efficacy, their exposure to cybercrime, overconfidence, and the cost of security products and services.

One of the European Commission's top priorities is the Digital Single Market[2], which aims to break down the barriers that prevent consumers in Europe from going digital with freedom. The first step to removing these barriers is to build a secure and trustworthy infrastructure. Policy actions are being devoted to reinforcing the adoption of standards that lead consumers to increase their security while online. Hence, it is important to approach security-by-design principles and PETs (privacy-enhancing technologies).

The present research contributes to this goal. It tests several warning messages that may persuade consumers to behave more securely while online, thus diminishing their chances of suffering a cyber-attack. These messages contain subtle differences in their wording, which are based on the literature of behavioural insights. The results presented in this report should help make consumers' behaviour more secure and should, ultimately, benefit e-commerce through a better understanding of what a secure ecosystem means.

This report presents the results from a test of the effect of ten different warning messages and assesses the policy implications that can be derived from these results.

1.1 Behavioural insights

Behavioural insights are increasingly popular policy tools for guiding citizens towards a desired behaviour (e.g. giving up smoking, saving energy saving, avoiding food waste) without enforcement. These insights can be applied to online behaviour (Pfleeger & Caputo, 2012; Rosoff, Cui, & John, 2013) and some of them have been tested in studies conducted by the Commission in support of EU policy. The most relevant insights on behaviour online for our study are described below.

- Overconfidence effect: people have a tendency to overestimate their knowledge and their own judgment due to high self-assurance (Pallier, *et al.,* 2002). This may increase risk-taking behaviour and lead individuals to believe wrongly that they control their own security (Nosic & Weber, 2010). Despite the risks of going online, these users may think that they will suffer no harm or that it is unlikely they will be

[1] https://ec.europa.eu/digital-single-market/en/news/europes-digital-progress-report-2016
[2] http://ec.europa.eu/priorities/digital-single-market/

attacked. In the context of security behaviour, users will ignore warning messages concerning their security online because they believe it is unlikely they will be the victims of a cyber-attack.

- Information overload: Individuals perceive that there are implicit costs in complying with security policies, such as increased cognitive load. Users will compute the extra effort that security mechanisms mean for them, and will compare it with the benefits obtained when they decide whether to comply or not (Beautement, Sasse & Wonham, 2009).

  Humans' capacity to process data and their attention span is limited. When there is too much information, users may feel that the harm that could be caused by ignoring this information does not warrant taking the time to read it. Information overload leads consumers to disregard relevant data when purchasing online (Jacoby, Speller & Berning, 1974; Scammon, 1977).

  Applied to security behaviour, this implies that long warning messages, which provide more information, will make users pay less rather than more attention to the message. Hypothesis 1 can be extracted from this insight, namely that *subjects who receive a long security message will behave less securely than subjects who receive a short security message.*

- Tailoring effect: the effect of personalizing messages has been widely developed in behavioural research. Information elicited from the individual is often used to create a personalized message. It can be more effective in stimulating a positive change in behaviour than generic interventions (Brinberg, Axelson & Price, 2000; Lancaster, T., & Stead, 2005). As regards security behaviour, a personalized warning message will attract users' attention more than a generic message. Hypothesis 2, therefore, is that *subjects who receive a personalized security message will behave more securely than subjects who receive one that is not personalized.*

- Social norms: norms are defined as rules, values and other criteria that are standardized as a consequence of the contact among individuals (Sheriff, 1936:3). Descriptive social norms tell us how others act in similar situations and shape our behaviour (Cialdini & Trost, 1998:152). The behaviour of the majority will have an effect on the individual due to social comparison, as individuals tend to avoid deviations from group consensus (Asch, 1956). Therefore, security warning messages based on descriptive norms should make users follow the majority. From this behavioural insight, two possible hypotheses can be tested:

  - *Hypothesis 3: subjects who receive a positive normative security message will behave more securely than subjects who receive a security message that makes no reference to social norms.*

  - *Hypothesis 4: subjects who receive a negative normative security message will behave less securely than subjects who receive a security message that makes no reference to social norms.*

- Gain vs loss framing effect: these effects refer to individuals' propensity to react in different ways depending on how the information is presented. The literature shows that when subjects are involved with the issue, a framed message will have a stronger effect than a message with no frame (Millar & Millar, 2000; Rothman, Martino, Bedell, Detweiler & Salovey, 1999; Rothman & Salovey, 1997).

  When comparing gain and loss-framing, it seems individuals will strongly prefer to avoid losses than to acquire gains of the same value (Kahneman & Tversky, 1979; Rothman, Salovey, Antone, Keough & Martin, 1993). Motivational theories explain this effect as a consequence of assigning stronger values to negative feelings than to

positive ones. However, this result depends on other factors such as how involved the subject is in the issue, or the level of risk of the behaviour itself (Banks, *et al.*, 1995; Maheswaran & Meyers-Levy, 1990; Meyers-Levy & Maheswaran, 2004).

Security warning messages framed in terms of potential losses will generate greater dread, and therefore lead to more secure behaviour, than warning messages framed in terms of potential gains. The related hypotheses can be formulated as follows:

- *Hypothesis 5: subjects who receive a loss-framed security message will behave more securely than subjects who receive a security message without such framing.*
- *Hypothesis 6: subjects who receive a gain-framed security message will not behave more securely than subjects who receive a security message without such framing.*

- Anthropomorphic character: including a humanoid figure in e-commerce contexts increases users' trust and perception of enjoyment. This results is confirmed when the human-like character looks like a traditional salesperson who offers users a helping hand (Heckman & Wobbrock, 2000; Qiu & Benbasat, 2009). However, researchers do not agree on the effects that an anthropomorphic figure may have. Some consider that the feeling of being observed may reduce the amount of personal information people disclose (Groom & Calo, 2011). As a consequence, using an anthropomorphic figure accompanied by a security message may push users to follow what the character asks them to do and behave safely.

  In security warning messages, anthropomorphic characters should heighten users' attention. Hypothesis 7 is the following: *subjects who receive a security message accompanied by an anthropomorphic character will behave more securely than subjects who see no character in the security message.*

- Visual indicator: visual signs that alert users about the level of online privacy and security may enhance their understanding of virtual notices. Users can use these signs as a faster way of obtaining information on the trustworthiness of the site they are visiting. Persuasive ambient technology has also been used to alert individuals, as it is easier to process than numerical feedback (Ham & Midden, 2010; Maan, Merkus, Ham & Midden, 2011). We therefore tested the hypothesis that *subjects receiving a security message accompanied by a visual indicator will behave more securely than subjects who receive no visual indicator at all (Hypothesis 8).*

2 Methodology

The study was conducted in Spain as a lab experiment with 600 participants (50% females[3]). Subjects were asked to make some online shopping decisions, and were assigned a quantity of money. The incentive for participating in the experiment was divided in two parts. The first part was a show-up fee that they would receive just for participating in the experiment. The other part depended on how secure their behaviour was during the purchasing process, and they were told this during the instructions at the beginning of the experiment. However, they were not informed about what would be considered secure when they were online: this depended solely on their previous knowledge. Incentives related with participants' performance during the experiment were required to simulate the risk they may take when going online. In the lab, it is not possible to introduce a virus in their computer or make them feel the risk of suffering a real cyber-attack. Since participants are not using their own computer, they may feel it is a safe environment.

After the instructions and before the purchase process began, subjects had to fill in a questionnaire with items about their risk aversion and impulsivity. These items were measured before we assigned the participants to the different experimental treatments, because we did not want to test the effect of the treatments on risk aversion and impulsivity, but to test the effect of risk aversion and impulsivity on the behavioural measures. At the end of the purchase process, they were also asked to complete a second questionnaire. It included questions related to trust in the online environment, and trust in the e-commerce provider. Here they could also report, from a list of behaviours, how far they could reduce the probability of suffering a cyber-attack by following the described behaviours. The purpose was to use the questionnaire as a measure of their previous knowledge to test if this had any effect on their performance during the purchase. All the results from analysing the data obtained in both questionnaires are described in the annexes.

2.1 Experimental procedure

The Ethics Committee on Experimental Behavioural Economics of the ERI-CES[4] approved this experiment, and confirmed that it adhered to the charter of ethics. The experiment was carried out between April and May 2015.

The study targeted 60 subjects per experimental treatment and tested a total of ten security messages based on the literature on behavioural insights online mentioned in Section 1.1.

Before the purchase process began, participants were asked some socio-demographic questions. In this part of the experiment, they had to provide their name, which would be used in the third treatment (*personalized message*) as explained below. Participants' names were not stored on the data base to guarantee their anonymity.

During the shopping process, subjects had to make several decisions that would affect their security, although they were not notified about the potential risks that these decisions entailed. The intention was to let them behave as they would in a non-experimental environment. They had to buy a real product (i.e. wallpaper) during the experiment. All the messages appeared as pop-ups in the centre of the screen before the

[3] Further information on socio-demographics can be found in the Annexes (see Table a).Note that the sample is skewed in education level, which may have potential implications for the interpretation of the results.

[4] http://www.lineex.es/home/index.php?lang=en

purchase process began. Participants had to close the pop-up window to continue with the experiment. The message was then placed in the upper part of the screen.

The ten experimental conditions were as follows:

1. **Control message:** this condition presented a pop-up message associated about navigating safely. We had two choices as regards the control condition: first, we could have chosen to present an environment with no security message, and second, an environment with a message that was as simple as possible. We discarded the first option as it differed in two aspects from the treatment groups: (1) inclusion of a message vs. no message at all; and (2) the nature of the message itself. If we had chosen the control with no message and had found an effect, we would not have been able to say if the effect was due to having a message (no matter the wording) or to the literature based wording of the particular message.

> Navigate safely.

2. **Long message:** this condition presented a pop-up with a longer neutral message about navigating safely. The rationale is that individuals would decide to ignore the message due to an 'information overload' effect.

> Browsing the Internet brings with it some risks. If you're seeing pop-up ads that won't go away, or you suddenly have a homepage that you know you didn't set, you may have an unwanted programme installed on your computer. There are some steps you can take to get rid of this programme and block similar ones from getting installed in the future. Phishing happens when someone tries to trick you to make you share information, usually through a fake website. Malicious software refers to harmful or unwanted software that is installed on your computer without your knowledge. Navigate safely.

3. **Personalized message:** this condition presented a neutral pop-up message about navigating safely. The message was personalized with the name of the subject. Subjects might feel that the message had been tailored to them and could pay more attention to it.

> 'Name of the subject', navigate safely.

4. **Positive normative message:** this condition presented a positive normative message together with the pop-up message about navigating safely. Social norms were expected to have an effect on participants' behaviour and make them follow what the majority do. They were expected to try to avoid deviating from the group norm.

> The majority of the Internet users in Spain are concerned about issues related with their online security. These users are taking steps to avoid suffering a cyber-attack.
>
> Navigate safely.

5. **Negative normative message:** this condition presented a negative normative message together with the pop-up message about navigating safely. This message followed the same logic as the previous treatment, but the message was negatively framed. Participants were expected to avoid deviating from the group norm, even if it was erroneous.

> The majority of the Internet users in Spain are not concerned about issues related with their online security. These users are not taking steps to avoid suffering a cyber-attack.
>
> Navigate safely.

6. **Gain-framed warning message:** this condition presented a gain-framed message together with the pop-up message about navigating safely. Gain-framed messages are more effective than messages with no frame, but the result also depends on the characteristics of the target subject.

> Navigate safely.
>
> If you do, you could win the maximum final endowment.

7. **Loss-framed warning message:** this condition presented a loss-framed message together with the pop-up message about navigating safely. Loss-framed messages are also more effective than messages with no frame, and when they are compared with the gain-framed messages, their effectiveness is usually greater.

> Navigate safely.
>
> If you don't, you could lose part of the final endowment.

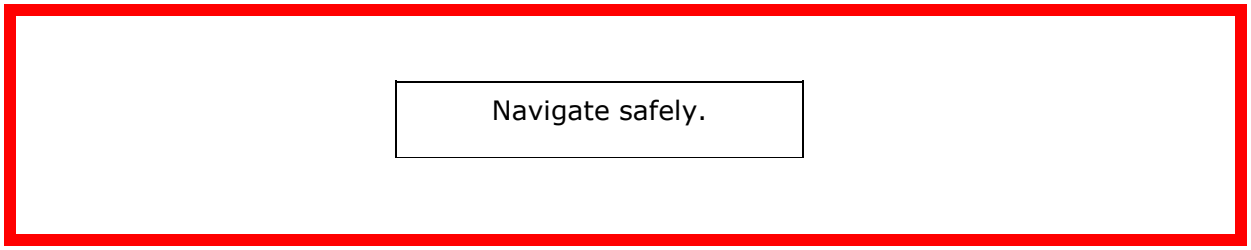
8. **Female anthropomorphic character:** this condition presented the same warning message as the control condition, but showed a female anthropomorphic character inside the pop-up message.

>  Navigate safely.

9. **Male anthropomorphic character**: this condition presented the same warning message as the control condition, but showed a male anthropomorphic character inside the pop-up message.

>  Navigate safely.

10. **Visual indicator:** this condition presented the same warning message as the control condition, but the screen of the e-commerce website was framed in red.



2.2 Behavioural output measures

The experiment measured five behavioural outcomes that have been listed as requirements if users are to maintain cyber security (Coventry, Briggs, Jeske & van Moorsel, 2014). We focused on those that are related to purchasing processes online and that could be tested during a behavioural experiment. Participants had to make the decisions sequentially as follows:

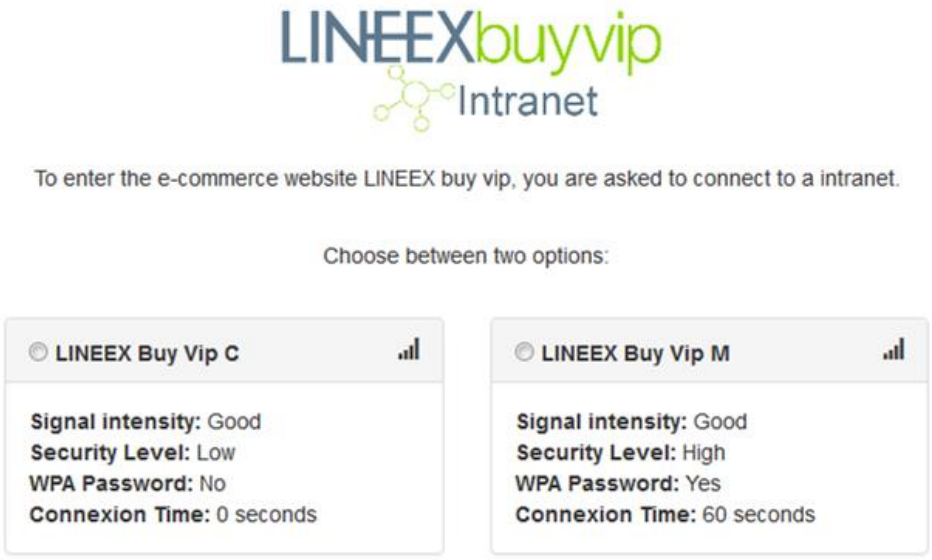
2.2.1 Secure connection

Before entering the e-commerce website, participants had to connect to a simulated intranet. They could choose between two options (presented randomly): a secure vs. an unsecured connection. The variable 'secure connection' was binary. It scored zero if subjects chose to behave unsafely and selected the unsecured option; and one if they made the secure choice. The options appeared randomly on the left or right hand side of the screen to avoid location having an effect on participants' decisions.

(a) Unsecured connection: this was an instant connection to a simulated intranet. Participants did not have to wait as the connection time was zero seconds and it did not require any password (see Figure 1).

(b) Secure connection: for this connection, participants had to wait 60 seconds and they had to type in the WPA password that was provided on the screen. Participants were made aware that it would take 1 minute to connect but the connection was secure. When they chose this option, they had to insert a WPA password that was provided to them on the same screen, which meant they had to make extra effort to behave securely.

Figure 1: Information provided on the screen for the intranet connection



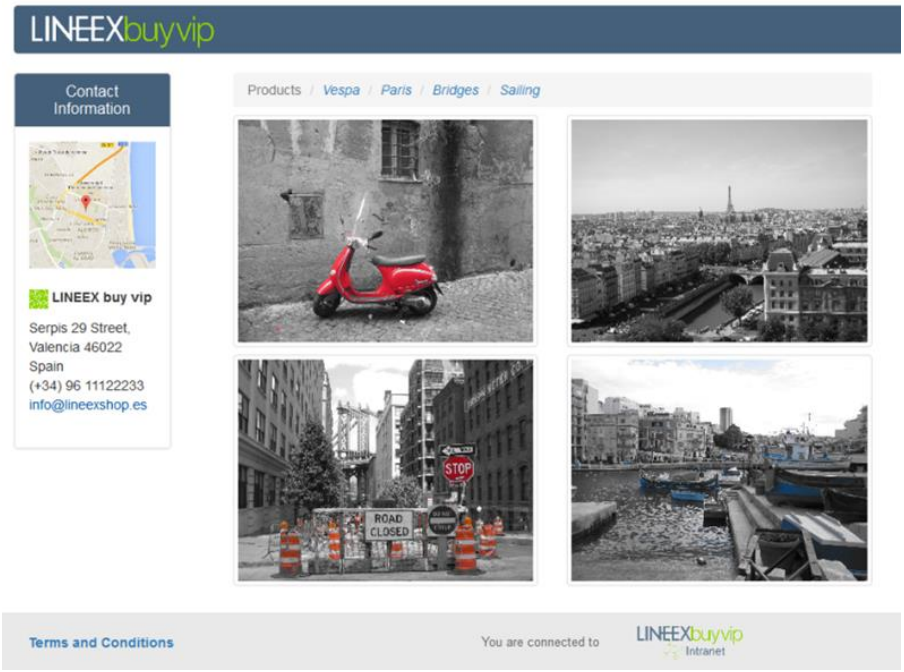
The justification is that choosing a secure option has to reflect the compliance budget that users weigh to make a decision (Beautement, Sasse & Wonham, 2009). They have to choose between spending some extra time in the connection, and getting the benefits of avoiding a cyber-attack and lose part of their incentive for participating in the experiment; or choosing the immediate connection and not having to wait, but increasing the risk of losing part of the incentive. This first decision was designed to reflect real world costs in terms of more stringent cybersecurity behaviours.

The next screen displayed a processing bar that charged during the connection. Below the bar, participants could see a button that allowed them to change to the unsecured but immediate connection, if they did not want to wait the whole minute. Including this possibility would let participants to change their mind as it might happen in the real world.

Once subjects had connected to the intranet, they were able to see the e-commerce website. The home page contained the company name and logo. In the bottom left-hand corner, there was a link to the terms and conditions. The link contained information about how the data would be managed, used and stored; rights of the user, and copyright information. All this information followed the Data Protection Directive 95/46/EC. Participants had to accept the terms and conditions during the sign-up process by clicking the button 'I agree to the Terms and Conditions'. However, it was not compulsory to open the link to the Terms and Conditions, so we expected a low rate of clicks on it.

The homepage was the gate for the subjects to start choosing products (see Figure 2). When a subject clicked on a product, a detailed page for that product opened. On this page, the subject could click on the button 'buy' to begin the process, or could go back to see any other product offered.

Figure 2: Homepage to choose the product



2.2.2 Password strength

Having decided which product to buy, the subject then had to register by creating a username and a password (see Figure 3). The behavioural measure 'password strength' was the strength level of the password chosen. The construct was measured according to the following seven common security parameters and scored between zero (if subjects did not meet any of the parameters) and seven (if they met all):

1. Minimum number of characters: 8
2. Minimum number of lower case characters: 2
3. Minimum number of upper case characters: 2
4. Minimum number of numeric digit characters: 2
5. Minimum number of special characters: 2
6. Boolean check whether password contains the username
7. Boolean check whether password contains the email

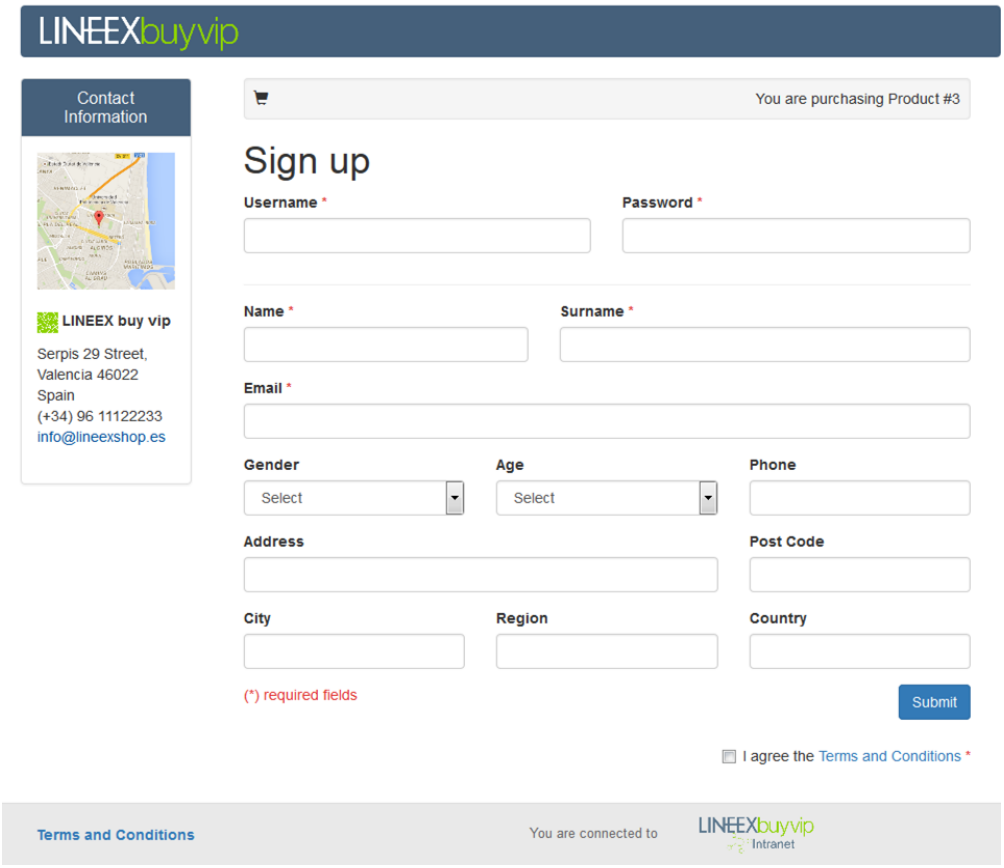
2.2.3 Information provided in the sign-up

During the registration process, after choosing the username and password, subjects were asked to provide some personal information (Figure 3). Participants had to provide the information marked with an asterisk (name, surname and email) in order to continue with the process, but they could choose whether or not to disclose the rest (gender, age, phone number, address, zip code, city, region and country). This is the usual information that is required in websites when registering or when making a purchase. e-Commerce providers find this information useful for sending targeted advertising. The behavioural measure 'sign-up info' scored between zero and eight, depending on the number of non-compulsory items that subjects disclosed. In this experiment, personal data disclosed by the participants was not recorded in order to guarantee their anonymity. The secure behaviour related to this outcome was to disclose only the information required (marked with the asterisk) to complete the purchase. However, this variable is limited as a

measure of secure behaviour because we cannot ensure that the information provided in the non-compulsory items was true.

From the moment subjects finished the registration until the end of the purchase process, the top right-hand side of the screen displayed the text 'Welcome' followed by their username, next to which was a button to log-out of the e-commerce website.

Figure 3: Sign-up page



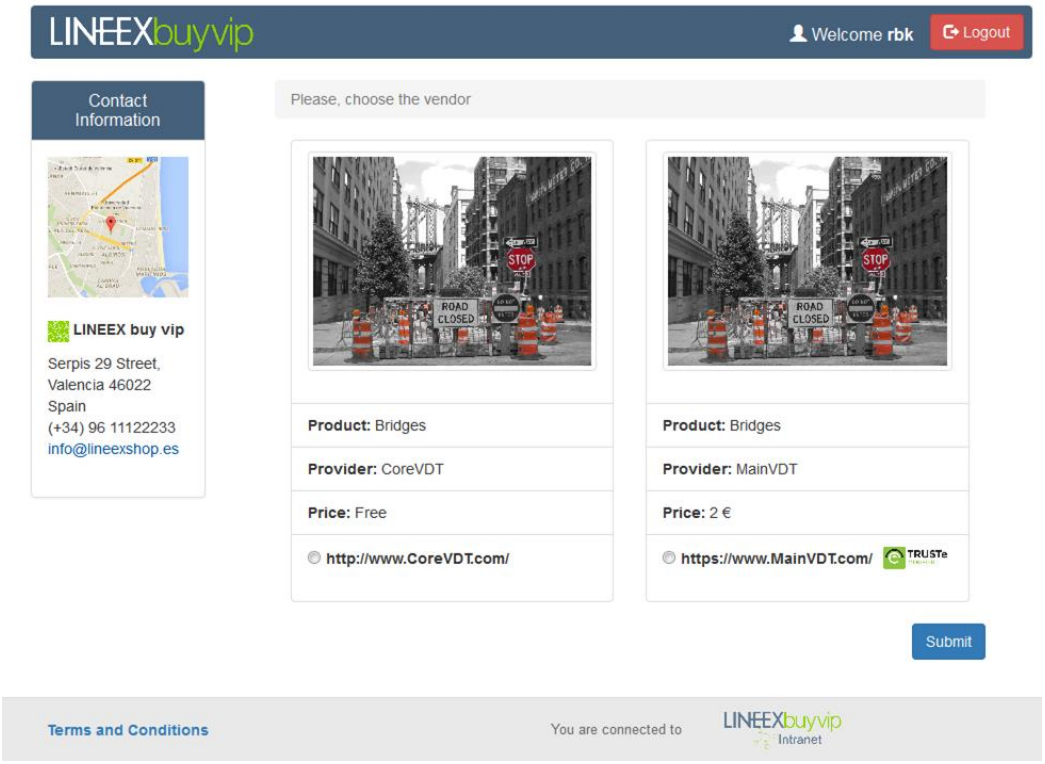
2.2.4 Trusted vendor

Once subjects had completed the registration process, confirmed their purchases and downloaded the product, they had to choose between two vendors. Both vendors offered the same product, but appeared on screen in varying orders (see Figure 4). The price offered by the first vendor for the product was zero (free). In this case, the link to download the product had no security signals (no image for an e-trusted site appeared). The simulated link for this supplier was http (Hypertext Transfer Protocol). The second vendor offered the product for €2, but the link to download it was of the type https (Hypertext Transfer Protocol Secure) and appeared next to an image indicating it was an e-trusted site. We gave different prices to the product depending on the security of the provider to reflect how in the online world users may obtain products for a zero price, but would have to pay a price related to their security.

The behavioural measure 'trusted vendor' scored zero if participants chose the unsecured option at zero price, and scored one if they chose the secure option from the trusted provider. After they had selected one of the vendors, they had to introduce a

credit card number, CVV and expiry date. A simulated credit card was provided to participants at the beginning of the experiment to give a more realistic feel to the experiment.

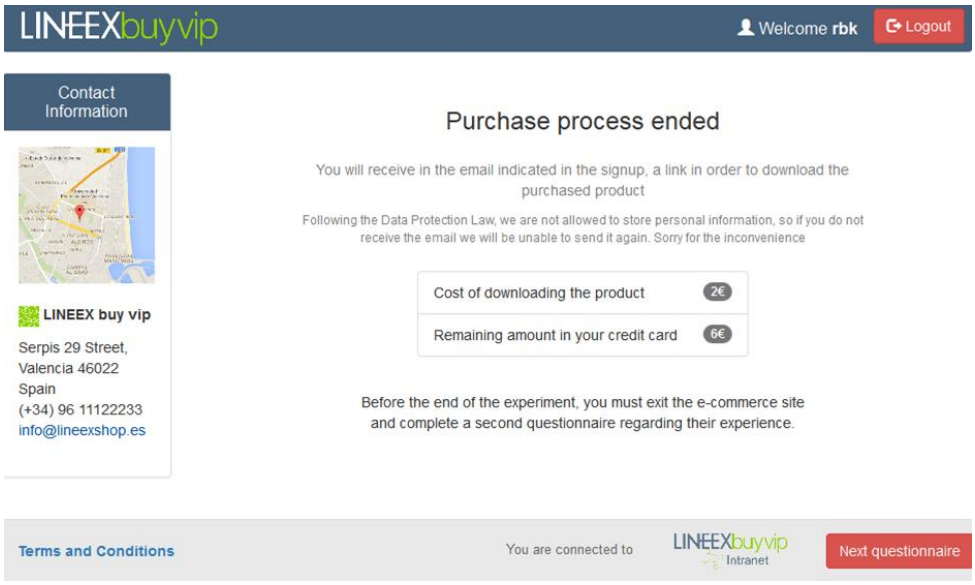
Figure 4: Selection of provider page



2.2.5 Log-out

Once subjects had completed the purchasing process, a new screen displayed information about the cost of the product purchased and how much they had left on their credit cards. A new button to the 'Next questionnaire' appeared at the bottom right-hand side of this screen. However, the secure behaviour was to log-out before continuing with the second questionnaire (see Figure 5). Participants were not directly guided to log-out, but they were asked to exit the e-commerce website and complete the second questionnaire. The behavioural measure 'log-out' scored zero if they decided to click on the next questionnaire button, and one if they chose the safest option and decided to log-out first.

Figure 5: Log-out page



3. Results

This section presents the results of the statistical analysis to test the hypotheses proposed. We provide information on the distribution of the decisions made by the participants in this experiment over the five behavioural measures under consideration.

In order to test the hypotheses proposed, we conducted a two-tailed t-test to see if the means of the control condition vs. the other conditions differed. We also added information regarding the subsamples (n=60), mean, standard deviation, and minimum and maximum score performed for each variable inside the group.

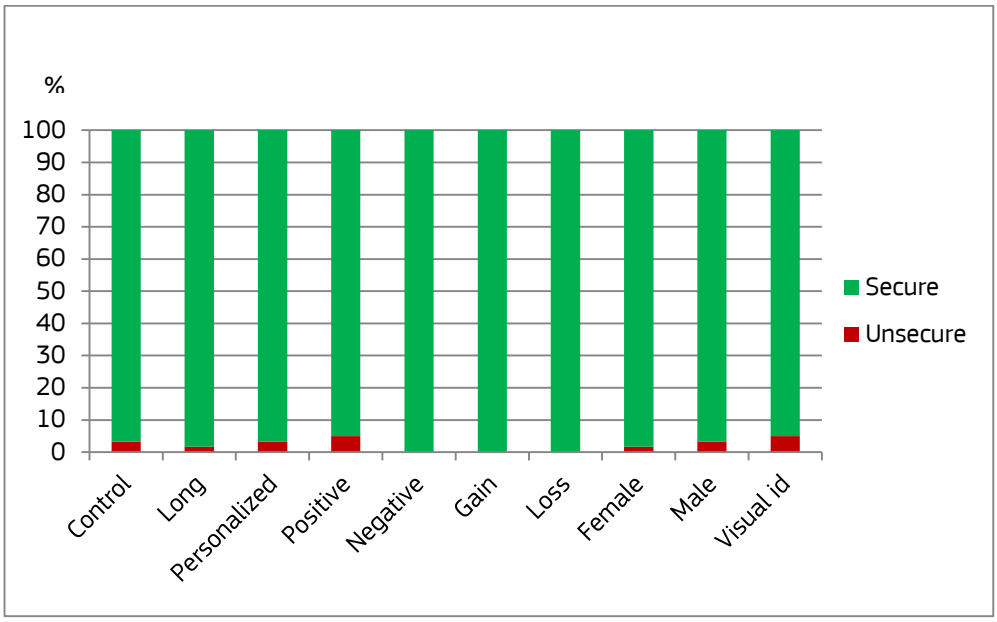
3.1 Secure connection

For this behavioural measure, we expected that subjects who received a long security message would choose the unsecured connection over the secure one compared with the control group, and would not wait the 60 seconds needed to connect securely.

For Hypotheses 2 to 8, the security message should have the opposite effect. Subjects in conditions three to ten should choose the secure connection over the unsecured one compared to the control group.

The first behavioural measure shows an unexpected trend. None of the treatments presented a significant difference with the control condition. Most of the subjects (98%) chose the secure connection, introduced the WPA password and waited for the more time-consuming option (see Figure 6). This means that none of the pop-up security messages was more effective than the control treatment, and that is why we have not included the results of the t-test in this subsection, as the groups did not differ. This decision about which connection to choose was the first one they had to make. Hence, the explanation for such a high rate of subjects choosing to behave securely and conducting to a ceiling effect could be that the warning message had a priming effect (Moon, 2000). As they had just seen a message warning them to navigate safely, just before they had to make the decision, the correct choice was very obvious at this point.

Figure 6: Subjects who chose the secure vs unsecured connection



3.2 Password strength

According to the hypotheses formulated, subjects who receive a long security message will choose less secure passwords that will comply with a lower number of security parameters, compared to subjects in the control group. However, if they are in conditions three to ten, they will do just the opposite and choose more secure passwords that will comply with a higher number of security parameters compared to the control group.

Results show that when subjects had to choose the username and password, the manipulated pop-up messages had no significant effect on their behaviour compared to the control group (see Table 1). Subjects chose passwords that complied on average with four out of the seven parameters that ensure a secure password (M=4.21, SD=1.01).

It is possible that participants did not have enough information on what we considered a strong password, as none of the treatments provided this information. Further research should test whether there is a significant difference when subjects already know how to create stronger passwords. Information on what a strong password is could be provided to them, to test if there is any change in their behaviour.

Table 1: Results of hypotheses testing for 'password strength'

Conditions	n	Mean	SD	Min - Max	t-test[#]
Control	60	4.17	0.94	3 – 6	NA
Long	60	4.40	1.18	1 – 6	0.2341
Personalized	60	4.30	0.96	2 – 6	0.4445
Positive	60	4.18	1.10	2 – 7	0.9290
Negative	60	4.28	1.01	3 – 6	0.5141
Gain	60	4.03	1.01	1 – 6	0.4555
Loss	60	4.27	1.02	3 – 7	0.5785
Female	60	4.22	0.99	2 – 6	0.7777
Male	60	4.07	0.99	2 – 6	0.5717
Visual indicator	60	4.22	0.94	2 – 6	0.7716

[#] *p*-value (Control vs. treatment). No significant effect of any of the treatments

3.3 Information provided in the sign-up

We expected that subjects who received a long security message would provide more information during the registering process in the e-commerce website compared to subjects in the control group, as they would feel overwhelmed by so much information and would not pay attention to the security message telling them to navigate safely. On

the other hand, in conditions three to ten, we expected that subjects would provide less personal information during the sign-up, compared to the control group.

However, there were two pop-up messages that aimed to make subjects disclose less information compared to the control treatment: the *long security message* and the one displaying a *male anthropomorphic character*.

Regarding the first result, contrary to what was expected, the long warning message made the participants behave more securely by providing less personal information. Hypothesis 1 (*subjects who receive a long security message will behave less securely than subjects who receive a short security message*) is not supported. One possible explanation for this result could be that the long message decreased the attention paid by subjects to the experiment, as the literature has suggested. Due to the information overload effect, they could feel overwhelmed by all the text they had to read and, as a consequence, end-up filling in fewer boxes on personal information in order to accelerate the purchase process.

The result obtained for the *male anthropomorphic character* supports Hypothesis 7 (*subjects who receive a security message accompanied by an anthropomorphic character will behave more securely than subjects who see no character in the security message.*) and enhances the evidence on how online social presence might decrease self-disclosure of personal information (Groom & Calo, 2011; Moon, 2000). The fact that the female character did not provide the same result, should be further investigated to find out whether there is any more evidence that shows a pattern regarding the effect of the character's gender.

The rest of the treatments showed no significant differences compared with the control in the t-test (see Table 2).

Table 2: Results of hypotheses testing for 'sign-up info'

Conditions	n	Mean	SD	Min - Max	t-test[#]
Control	60	6.47	2.66	0 – 8	NA
Long	60	**5.25**	3.35	0 – 8	**0.0297****
Personalized	60	5.85	3.19	0 – 8	0.2279
Positive	60	5.67	3.10	0 – 8	0.1319
Negative	60	6.08	3.02	0 – 8	0.4625
Gain	60	6.42	2.66	0 – 8	0.9182
Loss	60	5.78	3.15	0 – 8	0.2022
Female	60	6.70	2.47	0 – 8	0.6195
Male	60	**5.27**	3.40	0 – 8	**0.0334****
Light	60	5.60	3.06	0 – 8	0.1007

[#] *p*-value (Control vs. treatment)
*** $p<0.01$, ** $p<0.05$

3.4 Trusted vendor

Subjects who were shown the *long security message* were expected to choose untrusted vendors over trusted ones compared to the control group, and get the product for free instead of paying the €2 price. On the other hand, subjects assigned to treatments three to ten were expected to do the opposite and choose the trusted vendors over the untrusted ones, compared to the control condition.

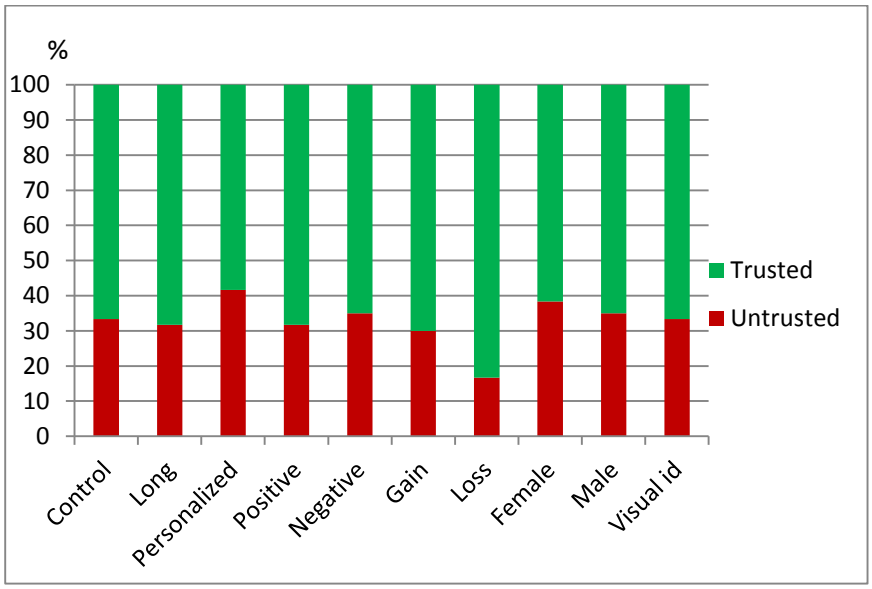
When subjects had to choose between the trusted and untrusted vendors, one of the warning messages showed a significant effect compared to the control condition (t-test *p*-value = 0.0352; see Table 3). A loss-framed warning message was more effective in making participants choose the trusted vendor: 83% of the participants in this condition chose the secure vendor, compared to 67% of subjects in the control condition (see Figure 7). A higher proportion of participants decided to buy the product from the trusted vendor in the loss-framed condition, despite the fact that they had to pay €2, instead of getting it for free and not spending any of their incentive. Hypothesis 5 is supported for this behavioural measure (*subjects who receive a loss-framed security message will behave more securely than subjects who receive a security message without such framing*).

Table 3: Results of hypotheses testing for 'trusted vendor'

Conditions	n	Mean	SD	Min - Max	t-test[#]
Control	60	0.67	0.48	0 – 1	NA
Long	60	0.68	0.47	0 – 1	0.8471
Personalized	60	0.58	0.50	0 - 1	0.3500
Positive	60	0.68	0.47	0 - 1	0.8471
Negative	60	0.65	0.48	0 - 1	0.8489
Gain	60	0.70	0.46	0 - 1	0.6976
Loss	60	**0.83**	0.38	0 - 1	**0.0352****
Female	60	0.62	0.49	0 - 1	0.5717
Male	60	0.65	0.48	0 - 1	0.8489
Light	60	0.67	0.48	0 - 1	1.0000

[#] *p*-value (Control vs. treatment)
*** $p<0.01$, ** $p<0.05$

Figure 7: Subjects who chose the trusted vs untrusted vendor



3.5 Log-out

For this particular security behaviour, the hypotheses formulated led us to expect that fewer subjects in the *long security message* condition would log-out than subjects in the control group. Subjects assigned to treatments three to ten would do the opposite and more of them would log out than participants in the control group.

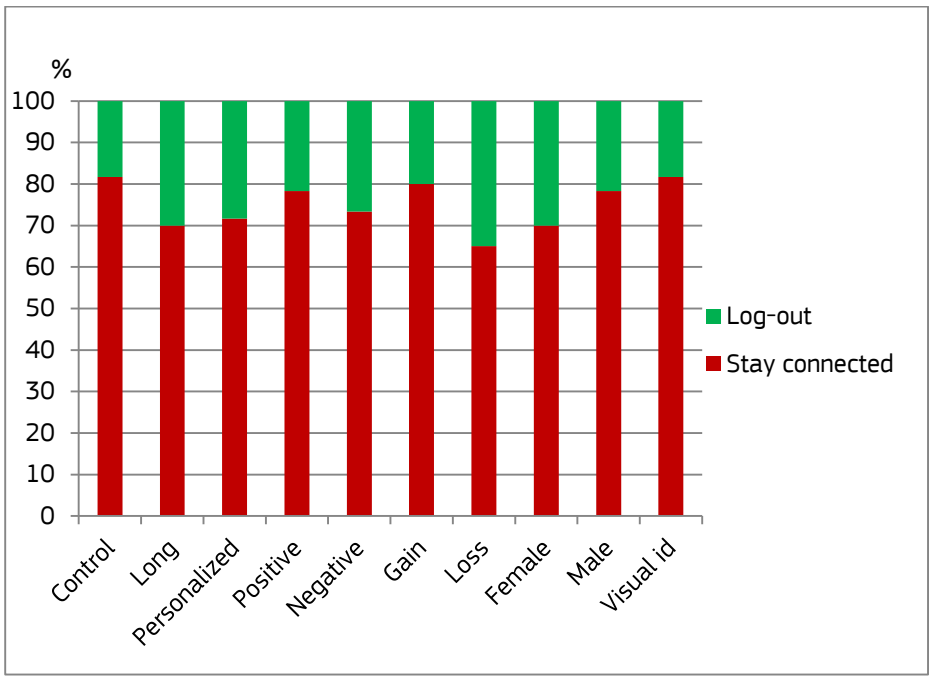
Results show that the last cyber secure behaviour measured was also influenced by one of the warning messages. As in the case of the trusted vendor, when subjects received a loss-framed warning message, there was a significant difference in their behaviour compared with the control condition (t-test *p*-value = 0.0393; see Table 4). Hypothesis 5 is also supported for this behavioural measure (*subjects who receive a loss-framed security message will behave more securely than subjects who receive a security message without such framing*). Up to 35% of the participants who were given the loss-framed warning message treatment chose the cyber-secure decision and log out before they clicked on the next questionnaire button, while only 18% of participants in the control condition made this same decision (see Figure 8). None of the other treatments showed any significant difference with the control condition.

Table 4: Results of hypotheses testing for 'log-out'

Conditions	n	Mean	SD	Min - Max	t-test[#]
Control	60	0.18	0.39	0 - 1	NA
Long	60	0.30	0.46	0 - 1	0.1378
Personalized	60	0.28	0.45	0 - 1	0.1985
Positive	60	0.22	0.42	0 - 1	0.6514
Negative	60	0.27	0.45	0 - 1	0.2782
Gain	60	0.20	0.40	0 - 1	0.8185
Loss	60	**0.35**	0.48	0 - 1	**0.0393****
Female	60	0.30	0.46	0 - 1	0.1378
Male	60	0.22	0.42	0 - 1	0.6514
Light	60	0.18	0.39	0 - 1	1.0000

[#] *p*-value (Control vs. treatment)
*** $p<0.01$, ** $p<0.05$

Figure 8: Subjects who logged-out vs stayed connected



3.6 Cybersecurity index

After conducting the data analysis, we found that security online is a complex concept that has various dimensions. In order to capture the maximum variability, we decided to build a new behavioural measure. This was a composite indicator, which included several individual indicators in a single index. This statistical measure was derived from the behavioural sources that seemed to be more reliable after analysing the results obtained in this experiment. The purpose was to obtain a new measure of cyber secure behaviour that captures several items of information, so it was composed as a multidimensional concept. All the indicators were equally weighted as there was no evidence that any of them should be reinforced. The formula used to compute the index was as follows:

$$Cybersecurity\ index = \frac{\frac{password\ strength}{7} + trusted\ vendor + \log - out}{3}$$

There are limitations to this index, as at the moment it only depicts a partial picture of what secure behaviour online really means. It could, however, be further developed in future research. The index includes information on four out of five of the mentioned behavioural measures that serve as indicators of secure behaviour. The first construct used in the lab experiment (*secure connection*) was excluded from the list of indicators as the data analysis showed that it was not a good measure of secure behaviour. For this first measure, we found that most of the participants were able to make the secure decision, probably because there was a priming effect (Forster & Davis, 1984) that lasted for the first few seconds after seeing the warning message, making this decision too obvious. The third construct (*sign-up info*) was also excluded from the cyber security index. The reason was that this measure did not capture whether the information that participants provided, in the case that they did so, was true or false. If the information had been true, it could have been risky to provide it; but if the information was false, the potential hazard disappeared.

Hypothesis testing shows that only one of the treatments seems to have a significant effect. Hypothesis 5 (subjects who receive a loss-framed security message will behave more securely than subjects who receive a security message without such framing) is corroborated (t-test p-value = 0.0115; see Table 5), which means that subjects who received the loss-framed warning messaged scored higher values in the cyber secure index.

Table 5: Results of hypotheses testing for 'cyber security index'

Conditions	n	Mean	SD	Min - Max	t-test[#]
Control	60	0.48	0.23	0.14 – 0.95	NA
Long	60	0.54	0.26	0.10 – 0.95	0.2132
Personalized	60	0.49	0.28	0.10 – 0.95	0.7973
Positive	60	0.50	0.24	0.14 – 0.95	0.6861
Negative	60	0.51	0.22	0.14 – 0.95	0.4975
Gain	60	0.49	0.22	0.05 – 0.95	0.8022
Loss	60	0.60	0.25	0.14 – 0.95	**0.0096*** **
Female	60	0.51	0.24	0.10 – 0.95	0.5675
Male	60	0.48	0.23	0.14 – 0.95	0.9850
Light	60	0.48	0.23	0.10 – 0.95	0.9552

[#] *p*-value (Control vs. treatment)

*** $p<0.01$, ** $p<0.05$

4. Conclusion

A number of findings can be extracted from this lab experiment. First, a loss-framed security message made subjects behave more securely by choosing a trusted vendor over an untrusted one and by logging out after purchasing on an e-commerce website. It also made subjects behave more securely online when cybersecurity was treated as a composite indicator build on three behavioural measures: choosing a trusted vendor, using secure passwords, and logging out.

This result confirms that the way in which security messages are framed is very important. Warning people about potential losses is an effective option for encouraging people to behave more securely. However, further research could search for differences depending on the level of risk of the behaviour itself.

Second, a long security message made subjects behave more securely online, as it made them disclose less personal information when signing-up to an e-commerce website[5]. The result was the opposite of what was expected (Hypothesis 1 stated that subjects receiving a long security message should behave *less* securely). Perhaps the information provided in the message required too much time and attention and reduced the time subjects wanted to spend on the registration process. The information overload effect could have worked in the opposite direction for this behavioural outcome compared to the other security measures.

Third, a security message accompanied by a male anthropomorphic character was also effective in leading consumers to disclose less personal information when signing up. In this case, the relationship between the variables went in the direction expected. A male anthropomorphic character led to less disclosure of information, confirming previous results in the literature (Groom & Calo, 2011; Moon, 2000). The reason why only the male, and not the female, character had an effect should be further investigated.

Fourth, the behavioural measure *password strength* showed no significant differences in any of the treatments compared to the control. This means that none of the security messages was effective in pushing the participants to use stronger passwords. This result may be related to users lacking information on what a strong password is, or lacking knowledge that could help them see the connection between stronger passwords and more secure behaviour online. This could be tested in subsequent studies by introducing further information into the security messages on (a) how using a stronger password can help increase the security level of online behaviour; and (b) indications of what makes a password strong.

In sum, the design of warning messages can affect online security behaviour – users are sensitive to it. This has policy implications for the design of security messages and any policy initiative expecting citizens to behave in a particular way. New initiatives, therefore, should include a controlled pilot phase to test their effectiveness before being rolled out.

---

[5] However, we cannot guarantee that those who provided more information at this stage did not lie. This was a limitation of this measure.

References

Asch, S. E. (1956). Studies of independence and conformity: I. A minority of one against a unanimous majority. *Psychological monographs: General and applied*, *70*(9), 1.

Banks, S. M., Salovey, P., Greener, S., Rothman, A. J., Moyer, A., Beauvais, J., & Epel, E. (1995). The effects of message framing on mammography utilization. *Health Psychology*, *14*(2), 178.

Beautement, A., Sasse, M. A., & Wonham, M. (2009). The compliance budget: managing security behaviour in organisations. In *Proceedings of the 2008 workshop on New security paradigms* (pp. 47-58). ACM.

Blais, A. R., & Weber, E. U. (2006). A domain-specific risk-taking (DOSPERT) scale for adult populations. *Judgment and Decision Making*, *1*(1).

Brinberg, D., Axelson, M. L., & Price, S. (2000). Changing food knowledge, food choice, and dietary fiber consumption by using tailored messages. *Appetite*, *35*(1), 35-43.

Cialdini, R. B., & Trost, M. R. (1998). Social influence: Social norms, conformity and compliance. In Gilbert, D. T. (Ed); Fiske, S. T. (Ed); Lindzey, G. (Ed). *The handbook of social psychology*, Vols. 1 and 2 (4th ed.)., (pp. 151-192). New York, NY, US: McGraw-Hill.

Coventry, L., Briggs, P., Jeske, D., & van Moorsel, A. (2014). Scene: A structured means for creating and evaluating behavioral nudges in a cybersecurity environment. In *Design, User Experience, and Usability. Theories, Methods, and Tools for Designing the User Experience* (pp. 229-239). Springer International Publishing.

Dickman, S. J. (1990). Functional and dysfunctional impulsivity: personality and cognitive correlates. Journal of Personality and Social Personality, 58(1), 95–102.

Dickman, S. J. (1993). Impulsivity and information processing. In W. Mc Cown, M. Shure, & J. Johnson (Eds.), The impulsive client: theory, research and treatment. Washington DC: American Psychological Association.

Dickman, S. J. (2000). Impulsivity, arousal and attention. Personality and Individual Differences, 28(3), 563–581.

Doney, P. M., & Cannon, J. P. (1997). An examination of the nature of trust in buyer-seller relationships. *The Journal of Marketing*, 35-51.

Forster, K. I., & Davis, C. (1984). Repetition priming and frequency attenuation in lexical access. *Journal of experimental psychology: Learning, Memory, and Cognition*, *10*(4), 680.

Groom, V., & Calo, M. R. (2011). Reversing the Privacy Paradox: An Experimental Study. *TPRC Conference proceedings, available at SSRN: http://ssrn.com/abstract=1993125*

Ham, J., & Midden, C. (2010). Ambient persuasive technology needs little cognitive effort: the differential effects of cognitive load on lighting feedback versus factual feedback. In *Persuasive Technology* (pp. 132-142). Springer Berlin Heidelberg.

Heckman, C. E., & Wobbrock, J. O. (2000, June). Put your best face forward: Anthropomorphic agents, e-commerce consumers, and the law. In *Proceedings of the fourth international conference on Autonomous agents* (pp. 435-442). ACM.

Jacoby, J., Speller, D. E., & Berning, C. K. (1974). Brand choice behavior as a function of information load: Replication and extension. *Journal of consumer research*, 33-42.

Jarvenpaa, S. L., Tractinsky, N., & Saarinen, L. (1999). Consumer trust in an internet store: a cross-cultural validation. *Journal of Computer-Mediated Communication*, *5*(2), 0-0.

Kahneman, D., & Tversky, A. (1979). Prospect theory: An analysis of decision under risk. *Econometrica*, *47*(2), 263-292.

Lancaster, T., & Stead, L. F. (2005). Self-help interventions for smoking cessation. *Cochrane Database Syst Rev*, *3*(3).

Maan, S., Merkus, B., Ham, J., & Midden, C. (2011). Making it not too obvious: the effect of ambient light feedback on space heating energy consumption. *Energy Efficiency*, *4*(2), 175-183.

Maheswaran, D., & Meyers-Levy, J. (1990). The influence of message framing and issue involvement. *Journal of Marketing Research*, 27, 361–367.

McKnight, D. H., Choudhury, V., & Kacmar, C. (2002). Developing and validating trust measures for e-commerce: An integrative typology. *Information systems research*, *13*(3), 334-359.

Meyers-Levy, J., & Maheswaran, D. (2004). Exploring message framing outcomes when systematic, heuristic, or both types of processing occur. Journal of Consumer Psychology, 14, 159–167.

Millar, M. G., & Millar, K. (2000). Promoting safe driving behaviors: The influence of message framing and issue involvement. *Journal of Applied Social Psychology*, 30, 853–856.

Moon, Y. (2000). Intimate exchanges: Using computers to elicit self-disclosure from consumers. *Journal of Consumer Research*, *26*(4), 323-339.

Nosic, A., & Weber, M. (2010). How riskily do I invest? The role of risk attitudes, risk perceptions, and overconfidence. *Decision Analysis*, 7(3), 282-301.

Pallier, G., Wilkinson, R., Danthiir, V., Kleitman, S., Knezevic, G., Stankov, L., & Roberts, R. D. (2002). The role of individual differences in the accuracy of confidence judgments. *The Journal of General Psychology*, 129(3), 257-299.

Pfleeger, S. L., & Caputo, D. D. (2012). Leveraging behavioral science to mitigate cyber security risk. *Computers & security*, *31*(4), 597-611.

Qiu, L., & Benbasat, I. (2009). Evaluating anthropomorphic product recommendation agents: A social relationship perspective to designing information systems. *Journal of Management Information Systems*, *25*(4), 145-182.

Rosoff, H., Cui, J., & John, R. S. (2013). Heuristics and biases in cyber security dilemmas. *Environment Systems and Decisions,* 33(4), 517-529.

Rothman, A. J., & Salovey, P. (1997). Shaping perceptions to motivate healthy behavior: The role of message framing. *Psychological Bulletin*, 121, 3–19.

Rothman, A. J., Martino, S. C., Bedell, B. T., Detweiler, J. B., & Salovey, P. (1999). The systematic influence of gain- and loss-framed messages on interest in and use of different types of health behavior. *Personality and Social Psychology Bulletin*, 25, 1355–1369.

Rothman, A. J., Salovey, P., Antone, C., Keough, K., & Martin, C. D. (1993). The influence of message framing on intentions to perform health behaviors. *Journal of Experimental Social Psychology*, *29*(5), 408-433.

Scammon, D. L. (1977). 'Information load' and consumers. *Journal of consumer research*, 148-155.

Sheriff (1936). *The psychology of social norms*. New York: Harper.

Weber, E. U., Blais, A. R., & Betz, N. E. (2002). A domain-specific risk-attitude scale: Measuring risk perceptions and risk behaviors. *Journal of behavioral decision making*, *15*(4), 263-290.

List of figures

List of tables

Annex I: Socio-demographics

The table below provides information on the socio-demographic distribution of the sample.

Table 6: Socio-demographic distribution

Variable	n	%
Gender		
Female	300	50
Male	300	50
Age		
18 – 34	239	39.83
35 and above	361	60.17
Education level		
No studies	5	0.83
Primary or Secondary Education	47	7.83
FP or High School	281	46.83
College Graduate	200	33.33
Postgraduate	55	9.17
PhD	11	1.83
No answer	1	0.17

Annex II: Risk aversion

The construct *risk aversion* was based on the Dospert scale (Blais & Weber, 2006; Weber, Blais & Betz, 2002) computed as an average of the scores that participants had on the 30 items scale. The latent variable presented high reliability with a Cronbach's alpha of 0.8380. Items are presented in Table 7. According to the scale, lower values in risk aversion mean that the subject is more risk averse.

Table 7: Risk aversion

Construct	Question	Answer
Risk aversion	For each of the following statements, please indicate the likelihood that you would engage in the described activity or behaviour if you were to find yourself in that situation. Provide a rating from Extremely Unlikely to Extremely Likely, using the following scale: 1. Admitting that your tastes are different from those of a friend. 2. Going camping in the wilderness. 3. Betting a day's income at a casino. 4. Investing 10% of your annual income in a moderate growth mutual fund. 5. Drinking heavily at a social function. 6. Taking some questionable deductions on your income tax return. 7. Disagreeing with an authority figure on a major issue. 8. Betting a day's income at a high-stake poker game. 9. Having an affair with a married man/woman. 10. Passing off somebody else's work as your own. 11. Going down a ski run that is beyond your ability. 12. Investing 5% of your annual income in a very speculative stock. 13. Going white-water rafting at high water in the spring. 14. Betting a day's income on the outcome of a sporting event. 15. Engaging in unprotected sex. 16. Revealing a friend's secret to someone else. 17. Driving a car without wearing a seat belt (reversed item). 18. Investing 10% of your annual income in a new business venture. 19. Taking a skydiving class. 20. Riding a motorcycle without a helmet. 21. Choosing a career that you truly enjoy over a more secure one. 22. Speaking your mind about an unpopular issue in a meeting at work. 23. Sunbathing without sunscreen. 24. Bungee jumping off a tall bridge. 25. Piloting a small plane. 26. Walking home alone at night in an unsafe area of town. 27. Moving to a city far away from your extended family. 28. Starting a new career in your mid-thirties. 29. Leaving your young children alone at home while running an errand. 30. Not returning a wallet you found that contains €200 (reversed item).	Scale from: [1] Extremely unlikely to [5] Extremely likely.

Table 8 tested the effect of *risk aversion* on the behavioural outcome *secure connection.* The results showed no effect of risk aversion on choosing a trusted connection.

Table 8: Anova to test the effect of *risk aversion* on *secure connection*

Source	Partial SS	Df	MS	F	Prob>F
Model	.018696005	3	.006232002	0.27	0.8456
Risk aversion	.018696005	3	.006232002	0.27	0.8456
Residual	13.6546373	596	.022910465		
Total	13.6733333	599	.022910465		
Number of obs = 600		R-squared = 0.0014			
Root MSE = .151362		Adj R-squared = -0.0037			

Table 9 test the effect of *risk aversion* on the behavioural outcome *password strength.* There is a significant effect of risk aversion on password strength. However, the analysis of variance provides information on whether there is significant effect but it does not specify the direction of this result. An ordered probit regression provides further information (coeff. = .3965756*; p-value* = 0.000) letting us know that, contrary to what we expected, more risk averse subjects will choose weaker passwords.

Table 9: Anova to test the effect of *risk aversion* on *password strength*

Source	Partial SS	Df	MS	F	Prob>F
Model	33.9190477	3	11.3063492	11.56	**0.0000*** **
Risk aversion	33.9190477	3	11.3063492	11.56	**0.0000*** **
Residual	582.774286	596	.977809204		
Total	616.693333	599	1.02953812		
Number of obs = 600		R-squared = 0.0550			
Root MSE = .988842		Adj R-squared = 0.0502			

*** $p<0.01$, ** $p<0.05$

Table 10 test the effect of *Risk aversion* on the behavioural outcome *sign-up info.* The results show no effect of risk aversion on the quantity of information that subjects provide during the sign-up process.

Table 10: Anova to test the effect of risk aversion on *sign-up info*

Source	Partial SS	Df	MS	F	Prob>F
Model	71.3571235	3	23.7857078	2.60	0.0511
Risk aversion	71.3571235	3	23.7857078	2.60	0.0511
Residual	5444.22788	596	9.13461053		
Total	5515.585	599	9.20798831		
Number of obs = 600		R-squared = 0.0129			
Root MSE = 3.02235		Adj R-squared = 0.0080			

Table 11 test the effect of *risk aversion* on the behavioural outcome *trusted vendor.* The results show no effect of risk aversion on choosing a trusted vendor.

Table 11: Anova to test the effect of *risk aversion* on *trusted vendor*

Source	Partial SS	Df	MS	F	Prob>F
Model	.939586678	3	.313195559	1.42	0.2345
Risk aversion	.939586678	3	.313195559	1.42	0.2345
Residual	131.033747	596	.21985528		
Total	131.973333	599	.22032276		
Number of obs = 600		R-squared = 0.0071			
Root MSE = .468887		Adj R-squared = 0.0021			

Table 12 tests the effect of *risk aversion* on the behavioural outcome *log-out.* The results show there is a significant effect of risk aversion on logging out. A probit regression provides information on the sign of the relationship (coeff. = .2887563; *p-value* = 0.005). Again, contrary to what we expected, subjects who are more risk averse will have a lower probability of logging out.

Table 12: Anova to test the effect of *risk aversion* on *log-out*

Source	Partial SS	Df	MS	F	Prob>F
Model	1.88298372	3	.627661241	3.38	**0.0180****
Risk aversion	1.88298372	3	.627661241	3.38	**0.0180****
Residual	110.617016	596	.185599021		
Total	112.5	599	.185599021		
Number of obs = 600		R-squared = 0.0167			
Root MSE = .468887		Adj R-squared = 0.0021			

*** $p<0.01$, ** $p<0.05$

Annex III: Impulsivity

Impulsivity was based on the 23-items Dickman's scale (Dickman, 1990; Dickman, 1993; Dickman, 2000). This scale distinguishes between functional and dysfunctional impulsivity as in Table 13. For this reason we have differentiated between two constructs: *functional impulsivity* and *dysfunctional impulsivity* (Table 14 and 15).

Table 13: Impulsivity

Construct	Question	Answer
Impulsivity	Please, answer to each of these questions with YES or NO: 1. I don't like to make decisions quickly, even simple decisions, such as choosing what to wear, or what to have for dinner (F - reversed). 2. I am good at taking advantage of unexpected opportunities, where you have to do something immediately or lose your chance (F) 3. Most of the time, I can put my thoughts into words very rapidly (F). 4. I am uncomfortable when I have to make up my mind rapidly (F - reversed). 5. I like to take part in really fast-paced conversations, where you don't have much time to think before you speak (F). 6. I don't like to do things quickly, even when I am doing something that is not very difficult (F - reversed). 7. I would enjoy working at a job that required me to make a lot of split-second decisions (F). 8. I like sports and games in which you have to choose your next move very quickly (F). 9. I have often missed out on opportunities because I couldn't make up my mind fast enough (F - reversed). 10. People have admired me because I can think quickly (F). 11. I try to avoid activities where you have to act without much time to think first (F - reversed). 12. I will often say whatever comes into my head without thinking first (D). 13. I enjoy working out problems slowly and carefully (D – reversed). 14. I frequently make appointments without thinking about whether I will be able to keep them (D). 15. I frequently buy things without thinking about whether or not I can really afford them (D). 16. I often make up my mind without taking the time to consider the situation from all angles (D). 17. Often, I don't spend enough time thinking over a situation before I act (D). 18. I often get into trouble because I don't think before I act (D). 19. Many times the plans I make don't work out because I haven't gone over them carefully enough in advance (D). 20. I rarely get involved in projects without first considering the potential problems (D - reversed). 21. Before making any important decision, I carefully weigh the pros and cons (D - reversed). 22. I am good at careful reasoning (D - reversed). 23. I often say and do things without considering the consequences (D).	Yes / No

The latent variables *functional impulsivity* and *dysfunctional impulsivity* presented high reliability (Tables 14 and 15).

Table 14: Functional impulsivity

Construct	Cronbach's alpha	Average interitem covariance
*Impulsivity_F (*a401- a411)	0.7886	.0604025

Table 15: Dysfunctional impulsivity

Construct	Cronbach's alpha	Average interitem covariance
*Impulsivity_D (*a412- a423)	0.7824	.0391679

Table 16 test the effect of *functional impulsivity* on the behavioural outcome *secure connection.* The results show no effect of functional impulsivity on choosing a trusted connection.

Table 16: Anova to test the effect of *functional impulsivity* on *secure connection*

Source	Partial SS	Df	MS	F	Prob>F
Model	.27166856	11	.02469714	1.08	0.3719
Functional impulsivity	.27166856	11	.02469714	1.08	0.3719
Residual	13.401665	588	.02279195		
Total	13.673333	599	.02282693		
Number of obs = 600		R-squared = 0.0199			
Root MSE = .15097		Adj R-squared = 0.0015			

Table 17 test the effect of *functional impulsivity* on the behavioural outcome *password strength.* The results show no effect.

Table 17: Anova to test the effect of *functional impulsivity* on *password strength*

Source	Partial SS	Df	MS	F	Prob>F
Model	14.199388	11	1.2908535	1.26	0.2442
Functional impulsivity	14.199388	11	1.2908535	1.26	0.2442
Residual	602.49394	588	1.0246496		
Total	616.69333	599	1.0295381		
Number of obs = 600		R-squared = 0.0230			
Root MSE = 1.01225		Adj R-squared = 0.0047			

*** $p<0.01$, ** $p<0.05$

Table 18 test the effect of *functional impulsivity* on the behavioural outcome *sign-up info.* The results show no effect functional impulsivity on the quantity of information that subjects provide during the sign-up process.

Table 18: Anova to test the effect of *functional impulsivity* on *sign-up info*

Source	Partial SS	Df	MS	F	Prob>F
Model	154.35381	11	14.032165	1.54	0.1134
Functional impulsivity	154.35381	11	14.032165	1.54	0.1134
Residual	5361.2312	588	9.1177401		
Total	5515.585	599	9.2079883		
Number of obs = 600		R-squared = 0.0280			
Root MSE = 3.01956		Adj R-squared = 0.0098			

Table 19 test the effect of *functional impulsivity* on the behavioural outcome *trusted vendor.* The results show a significant effect. A probit regression provides information on the sign of the relationship (coeff. = .0548987; *p-value* = 0.009). Subjects who are more functionally impulsive will have a higher probability of choosing a trusted vendor when purchasing online, hence they will have a higher probability of behaving securely.

Table 19: Anova to test the effect of *functional impulsivity* on *trusted vendor*

Source	Partial SS	Df	MS	F	Prob>F
Model	5.4035887	11	.49123534	2.28	**0.0099**
Functional impulsivity	5.4035887	11	.49123534	2.28	**0.0099**
Residual	126.56974	588	.21525467		
Total	131.97333	599	.22032276		
Number of obs = 600		R-squared = 0.0409			
Root MSE = .463955		Adj R-squared = 0.0230			

*** $p<0.01$, ** $p<0.05$

Table 20 test the effect of *functional impulsivity* on the behavioural outcome *log-out.* The results show no effect of functional impulsivity on logging out.

Table 20: Anova to test the effect of functional impulsivity on *log-out*

Source	Partial SS	Df	MS	F	Prob>F
Model	1.6689146	11	.15171951	0.80	0.6353
Functional impulsivity	1.6689146	11	.15171951	0.80	0.6353
Residual	110.83109	588	.18848824		
Total	112.5	599	.18781302		
Number of obs = 600		R-squared = 0.0148			
Root MSE = .434152		Adj R-squared = -0.0036			

*** $p<0.01$, ** $p<0.05$

Annex IV: Trust in the online environment

The construct *trust online* was computed as an average of the scores that participants had on a scale of 14 items (McKnight, Choudhury & Kacmar, 2002). The latent variable presented excellent reliability with a Cronbach's alpha of 0.9277 and average interitem covariance of 0.5207981. Items are presented in Table 21.

Table 21: Trust in the online environment

Construct	Question	Answer
Trust online	Please, choose in the table below the level of agreement or disagreement with the statements listed: 1. I am comfortable making purchases or other activities on the Internet 2. I feel that most Internet vendors would act in a customers' best interest. 3. If a customer required help, most Internet vendors would do their best to help. 4. Most Internet vendors are interested in customer wellbeing, not just their own wellbeing. 5. I am comfortable relying on Internet vendors to meet their obligations. 6. I feel fine doing business on the Internet since Internet vendors generally fulfil their agreements. 7. I always feel confident that I can rely on Internet vendors to do their part when I interact with them. 8. In general, most Internet vendors are competent at serving their customers. 9. Most Internet vendors do a capable job at meeting customer needs. 10. I feel that most Internet vendors are good at what they do. 11. The Internet has enough safeguards to make me feel comfortable using it to transact personal business. 12. I feel assured that legal and technological structures adequately protect me from problems on the Internet. 13. I feel confident that encryption and other technological advances on the Internet make it safe for me to do business there. 14. In general, the Internet is now a robust and safe environment in which to transact business.	Scale from [1] Strongly agree [5] Strongly disagree.

Table 22 shows the effect of *trust in the online environment* on the behavioural outcome *secure connection.* The results indicate an effect of trust in the online environment on choosing a trusted connection. However, further probit regressions do not confirm this effect (p=0.335).

Table 22: Anova to test the effect of *trust in the online environment* on *secure connection*

Source	Partial SS	Df	MS	F	Prob>F
Model	.480485362	4	.120121341	5.42	**0.0003**
Trust in the online environment	.480485362	4	.120121341	5.42	**0.0003**
Residual	13.192848	595	.022172854		
Total	13.673333	599	.02282693		
Number of obs = 600		R-squared = 0.0351			
Root MSE = .148906		Adj R-squared = 0.0287			

Table 23 shows the effect of *trust in the online environment* on the behavioural outcome *assword strength.* The results show no effect.

Table 23: Anova to test the effect of *trust in the online environment* on *password strength*

Source	Partial SS	Df	MS	F	Prob>F
Model	4.4011024	4	1.1002756	1.07	0.3709
Trust in the online environment	4.4011024	4	1.1002756	1.07	0.3709
Residual	612.29223	595	1.0290626		
Total	616.69333	599	1.0295381		
Number of obs = 600		R-squared = 0.0071			
Root MSE = 1.01443		Adj R-squared = 0.0005			

Table 24 test the effect of *trust in the online environment* on the behavioural outcome *sign-up info.* The results show an effect of trust in the online environment on the amount of information participants provided during the sign-up process. A probit regression provides information on the sign of the relationship (coeff. = .1960472; *p-value* = 0.023). Subjects who show greater trust in the online environment disclose more personal information at the sign-up stage.

Table 24: Anova to test the effect of *trust in the online environment* on *sign-up info*

Source	Partial SS	Df	MS	F	Prob>F
Model	104.2351	4	26.058775	2.87	**0.0227**
Trust in the online environment	104.2351	4	26.058775	2.87	**0.0227**
Residual	5411.3499	595	9.0947057		
Total	5515.585	599	9.2079883		
Number of obs = 600		R-squared = 0.0189			
Root MSE = 3.01574		Adj R-squared = 0.0123			

Table 25 test the effect of *trust in the online environment* on the behavioural outcome *trusted vendor.* The results show no effect of trust in the online environment on choosing a trusted vendor.

Table 25: Anova to test the effect of *trust in the online environment* on *trusted vendor*

Source	Partial SS	Df	MS	F	Prob>F
Model	.53648328	4	.13412082	0.61	0.6576
Trust in the online environment	.53648328	4	.13412082	0.61	0.6576
Residual	131.43685	595	.22090227		
Total	131.97333	599	.22032276		
Number of obs = 600		R-squared = 0.0041			
Root MSE = .470002		Adj R-squared = -0.0026			

Table 26 test the effect of *trust in the online environment* on the behavioural outcome *log-out.* The results show no effect of trust in the online environment on logging out.

Table 26: Anova to test the effect of trust in the online environment on *log-out*

Source	Partial SS	Df	MS	F	Prob>F
Model	1.4529485	4	.36323713	1.95	0.1013
Trust in the online environment	1.4529485	4	.36323713	1.95	0.1013
Residual	111.04705	595	.1866337		
Total	112.5	599	.18781302		
Number of obs = 600		R-squared = 0.0129			
Root MSE = .432011		Adj R-squared = 0.0063			

Annex V: Trust in the e-commerce provider

The construct *trust provider* was computed as an average of the scores that participants had on a scale of 10 items (Doney & Cannon, 1997; Jarvenpaa, Tractinsky & Saarinen, 1999; McKnight, Choudhury & Kacmar, 2002). The latent variable presented high reliability (Cronbach's alpha = 0.9277; Average interitem covariance = 0.5207981). Items are presented in Table 27.

Table 27: Trust in the e-commerce provider

Construct	Question	Answer
Trust provider	Please, choose in the table below the level of agreement or disagreement with the statements listed: 1. I believe that LINEEX Buyvip would act in my best interest. 2. If required help, LINEEX Buyvip would do its best to help me. 3. LINEEX Buyvip is interested in my wellbeing, not just its own. 4. LINEEX Buyvip is truthful in its dealings with me. 5. LINEEX Buyvip is sincere and genuine. 6. This e-commerce vendor is trustworthy. 7. This e-commerce vendor provides reliable information. 8. This e-commerce vendor keeps promises and commitments. 9. This e-commerce vendor's behaviour meets my expectations. 10. I find it necessary to be cautious with this store.	Scale from [1] Strongly agree [5] Strongly disagree.

Table 28 shows the results from analysing the effect of the treatments on the level of trust in the e-commerce provider. There is no effect of any of the treatments on *trust in the e-commerce provider*, compared with the control group.

Table 28: Ordered probit regression to test the effect of the treatments on trust in the e-commerce provider

Treatments	Coef.	Std.Err	z	P>|z|	[95% Conf.	Interval]
Long	.0195332	.1955404	0.10	0.920	-.3637189	.4027852
Personalized	-.1738157	195574	-0.89	0.374	-.5571337	.2095024
Positive	.4014195	.1969604	2.04	0.042	.0153842	.7874548
Negative	.220492	.1964318	1.12	0.262	-.1645072	.6054912
Gain	.1344993	.1961667	0.69	0.493	-.2499805	.518979
Loss	.1786775	.1962899	0.91	0.363	-.2060436	.5633986
Female	.0688717	.1960762	0.35	0.725	-.3154306	.4531741
Male	.0602622	.1956386	0.31	0.758	-.3231823	.4437068
Visual id	-.0427219	.1957885	-0.22	0.827	-.4264604	.3410165
Number of obs = 600		LR chi2(9) = 11.58				
Prob > chi2 = 0.2383		Log likelihood = -718.80957			Pseudo R2 =	0.0080

Annex VI: Knowledge

Table 29 and 30 give information about the items included in the post-purchase questionnaire that were related with knowledge. In the subsequent pages we have included the results from analysing the effect of treatments on knowledge related items, and the effect of knowledge related items on the behavioural outcomes measured.

Table 29: Perceived knowledge

Construct	Question	Answer
Perceived knowledge	How well informed do you feel about the risks of cybercrime?	1. Not at all informed. 2. Not very well informed. 3. Somewhat informed. 4. Fairly well informed. 5. Very well informed.

Table 30: Knowledge

Construct	Question	Answer
Knowledge	Which of the following behaviours do you think can help you prevent from being attacked while online?	Provide a rating from [1] It won't reduce my risk at all to [5] It will reduce my risk extremely
Knowledge_safe	Connecting to a trusted connection.	
Knowledge_pswd1	Using a strong password.	
Knowledge_pswd2	Changing your password frequently.	
Knowledge_pswd3	Avoid using the same password for different sites.	
Knowledge_signup	Providing minimum information.	
Knowledge_trust	Connecting to a trusted site.	
Knowledge_logout	Logging out.	
Knowledge_soft1	Using anti-virus software and firewalls.	
Knowledge_soft2	Updating software to the latest version.	
Knowledge_public	Avoiding access to my personal accounts in public places.	

The next table shows there is no effect of any of the treatment groups on *perceived knowledge*, compared with the control group (i.e. none of the treatments made subjects feel more or less informed about the risks of cybercrime).

Table 31: Ordered probit regression to test the effect of the treatments on *perceived knowledge*

TTreatments	Coef.	Std.Err	z	P>|z|	[95% Conf.	Interval]
Long	.2332664	.1939215	1.20	0.229	-.1468127	.6133456
Personalized	-.2587961	.193495	-1.34	0.181	-.6380392	.1204471
Positive	-.0556485	.1937408	-0.29	0.774	-.4353735	.3240764
Negative	-.1260651	.1931002	-0.65	0.514	-.5045346	.2524044
Gain	-.0031957	.1934928	-0.02	0.987	-.3824346	.3760432
Loss	.0868073	.1930783	0.45	0.653	-.2916192	.4652339
Female	.0374471	.1932064	0.19	0.846	-.3412304	.4161246
Male	-.0181604	.1933668	-0.09	0.925	-.3971525	.3608317
Visual id	.0527654	.1931794	0.27	0.785	-.3258593	.4313901

Number of obs = 600 LR chi2(9) = 8.08
Prob > chi2 = 0.5260 Log likelihood = -789.60292 Pseudo R2 = 0.0051

Table 32 shows no effect of treatments on the item *knowledge_safe* compared to the control group.

Table 32: Ordered probit regression to test the effect of the treatments on *knowledge_safe*

Treatments	Coef.	Std.Err	z	P>|z|	[95% Conf.	Interval]
Long	.0604554	.2032446	0.30	0.766	-.3378966	.4588074
Personalized	.0709599	.2036128	0.35	0.727	-.3281138	.4700335
Positive	.2076836	.2047389	1.01	0.310	-.1935973	.6089645
Negative	.0673573	.203257	0.33	0.740	-.3310191	.4657337
Gain	.2363826	.2059386	1.15	0.251	-.1672496	.6400148
Loss	.2308275	.2055136	1.12	0.261	-.1719717	. 6336267
Female	-.1210464	.2015109	-0.60	0.548	-.5160004	. 2739077
Male	-.2338345	.2003818	-1.17	0.243	-.6265756	.1589066
Visual id	.1249636	2039358	0.61	0.540	-.2747431	.5246704
Number of obs = 600		LR chi2(9) = 10.17				
Prob > chi2 = 0.3369		Log likelihood = -672.82244			Pseudo R2 =	0.0075

Table 33 shows no effect of treatments on the item *knowledge_pswd1* compared to the control group.

Table 33: Ordered probit regression to test the effect of the treatments on *knowledge_pswd1*

Treatments	Coef.	Std.Err	z	P>|z|	[95% Conf.	Interval]
Long	.0990497	.2028759	0.49	0.625	-.2985798	.4966792
Personalized	.1893817	.2049022	0.92	0.355	-.2122192	.5909826
Positive	.2507903	.2053491	1.22	0.222	-.1516866	.6532672
Negative	.0918029	.2022107	0.45	0.650	-.3045228	.4881285
Gain	.3153935	.2070763	1.52	0.128	-.0904685	.7212555
Loss	.260954	.2053197	1.27	0.204	-.1414651	.6633731
Female	-.1421162	.2001148	-0.71	0.478	-.5343339	.2501016
Male	-.2058515	.1998837	-1.03	0.303	-.5976164	.1859134
Visual id	.0407208	.2019394	0.20	0.840	-.3550732	. 4365147
Number of obs = 600		LR chi2(9) = 12.86				
Prob > chi2 = 0.1689		Log likelihood = -685.54666			Pseudo R2 =	0.0093

Table 34 shows no effect of treatments on the item *knowledge_pswd2* compared to the control group.

Table 34: Ordered probit regression to test the effect of the treatments on *knowledge_pswd2*

Treatments	Coef.	Std.Err	z	P>|z|	[95% Conf.	Interval]
Long	.2230119	.2040504	1.09	0.274	-.1769195	.6229434
Personalized	.0243323	.2018169	0.12	0.904	-.3712215	.4198862
Positive	.0613403	.2019032	0.30	0.761	-.3343827	.4570634
Negative	-.1089494	.2003389	-0.54	0.587	-.5016064	.2837077
Gain	.2225366	.2047026	1.09	0.277	-.178673	.6237462
Loss	.2257531	.2047311	1.10	0.270	-.1755126	.6270187
Female	.0921139	.2026401	0.45	0.649	-.3050535	.4892813
Male	.0549412	.201563	0.27	0.785	-.3401149	.4499974
Visual id	.1075741	.2023848	0.53	0.595	-.2890928	.504241
Number of obs = 600		LR chi2(9) = 5.17				
Prob > chi2 = 0.8193		Log likelihood = -695.57447			Pseudo R2 =	0.0037

Table 35 shows that there is an effect of several treatments on the item of treatments on the item *knowledge_pswd3*. The *negative normative*, *gain and loss-framed*, *female anthropomorphic character* and the *visual indicator* treatments have a positive effect on *knowledge_pswd3* compared to the control group.

Table 35: Ordered probit regression to test the effect of the treatments on *knowledge_pswd3*

Treatments	Coef.	Std.Err	z	P>|z|	[95% Conf.	Interval]
Long	.310477	.2024902	1.53	0.125	-.0863965	.7073505
Personalized	.1721796	.2006975	0.86	0.391	-.2211803	.5655394
Positive	.2085422	.2003375	1.04	0.298	-.184112	.6011964
Negative	.4130974	.203572	2.03	**0.042**	.0141036	.8120912
Gain	.4130974	.203572	2.03	**0.042**	.0141036	.8120912
Loss	.5554429	.2071574	2.68	**0.007**	.1494217	.961464
Female	.4823346	.205191	2.35	**0.019**	.0801676	.8845015
Male	.1569392	.1993777	0.79	0.431	-.2338339	.5477122
Visual id	.4377518	.2039213	2.15	**0.032**	.0380734	.8374301
Number of obs = 600		LR chi2(9) = 13.10				
Prob > chi2 = 0.1583		Log likelihood = -698.99083			Pseudo R2 =	0.0093

Table 36 shows no effect of treatments on the item *knowledge_signup* compared to the control group.

Table 36: Ordered probit regression to test the effect of the treatments on *knowledge_signup*

Treatments	Coef.	Std.Err	z	P>|z|	[95% Conf.	Interval]
Long	-.1629619	.1962479	-0.83	0.406	-.5476008	.2216769
Personalized	-.0715575	.1973754	-0.36	0.717	-.4584061	.3152911
Positive	-.0285881	.1969752	-0.15	0.885	-.4146524	.3574763
Negative	.0562473	.1984672	0.28	0.777	-.3327413	.445236
Gain	-.0551609	.1968491	-0.28	0.779	-.440978	.3306563
Loss	.3072582	.2009564	1.53	0.126	-.0866092	.7011256
Female	.2070848	.2009194	1.03	0.303	-.18671	.6008797
Male	-.0216561	.1976419	-0.11	0.913	-.4090272	.365715
Visual id	.2428927	.2000433	1.21	0.225	-.1491851	.6349704
Number of obs = 600		LR chi2(9) = 10.56				
Prob > chi2 = 0.3074		Log likelihood = -784.12873			Pseudo R2 =	0.0067

Table 37 shows that *gain and loss-framed security messages* have a positive effect on the item *knowledge_trust* compared to the control group.

Table 37: Ordered probit regression to test the effect of the treatments on *knowledge_trust*

Treatments	Coef.	Std.Err	z	P>|z|	[95% Conf.	Interval]
Long	.1280212	.2062597	0.62	0.535	-.2762404	.5322829
Personalized	.1761076	.2074243	0.85	0.396	-.2304365	.5826517
Positive	.3327227	.2100281	1.58	0.113	-.0789248	.7443701
Negative	.0996481	.205528	0.48	0.628	-.3031795	.5024757
Gain	.5145198	.2147816	2.40	**0.017**	.0935555	.935484
Loss	.4885981	.2134252	2.29	**0.022**	.0702923	.9069038
Female	.034575	.2045424	0.17	0.866	-.3663207	.4354707
Male	.1284136	.2058505	0.62	0.533	-.2750459	.5318731
Visual id	.1773313	.2066422	0.86	0.391	-.22768	.5823425
Number of obs = 600		LR chi2(9) = 12.35				
Prob > chi2 = 0.1942		Log likelihood = -607.67649			Pseudo R2 =	0.0101

Table 38 shows that the *personalized security message* has a positive effect on the item *knowledge_logout* compared to the control group.

Table 38: Ordered probit regression to test the effect of the treatments on *knowledge_logout*

Treatments	Coef.	Std.Err	z	P>|z|	[95% Conf.	Interval]
Long	.0751808	.2015535	0.37	0.709	-.3198569	.4702184
Personalized	.4701044	.2105141	2.23	**0.026**	.0575043	.8827045
Positive	.2891167	.2056824	1.41	0.160	-.1140134	.6922468
Negative	.2941972	.2054425	1.43	0.152	-.1084627	.696857
Gain	.3483072	.2085126	1.67	0.095	-.06037	.7569844
Loss	.3947567	.2078651	1.90	0.058	-.0126515	.8021649
Female	2980087	.2057603	1.45	0.148	-.1052742	.7012915
Male	.0362993	.2012758	0.18	0.857	-.358194	.4307926
Visual id	.017717	.2009849	0.09	0.930	-.3762062	.4116402
Number of obs = 600		LR chi2(9) = 12.45				
Prob > chi2 = 0.1893		Log likelihood = -685.41583			Pseudo R2 = 0.0090	

Table 39 shows no effect of treatments on the item *knowledge_soft1* compared to the control group.

Table 39: Ordered probit regression to test the effect of the treatments on *knowledge_soft1*

Treatments	Coef.	Std.Err	z	P>|z|	[95% Conf.	Interval]
Long	-.1062479	.2108163	-0.50	0.614	-.5194403	.3069445
Personalized	.056772	.2134403	0.27	0.790	-.3615632	.4751072
Positive	-.2312815	.2081436	-1.11	0.266	-.6392354	.1766724
Negative	-.2078111	.2081875	-1.00	0.318	-.6158512	.200229
Gain	.0617064	.213286	0.29	0.772	-.3563266	.4797393
Loss	-.0014358	.2122635	-0.01	0.995	-.4174646	.4145931
Female	-.1168473	.2088313	-0.56	0.576	-.5261491	.2924545
Male	-.1285453	.2088715	-0.62	0.538	-.5379259	.2808353
Visual id	.04334	.2128888	0.20	0.839	-.3739144	.4605943
Number of obs = 600		LR chi2(9) = 4.88				
Prob > chi2 = 0.8449		Log likelihood = -642.60538			Pseudo R2 = 0.0038	

Table 40 shows no effect of treatments on the item *knowledge_soft2* compared to the control group.

Table 40: Ordered probit regression to test the effect of the treatments on *knowledge_soft2*

Treatments	**Coef.**	**Std.Err**	**z**	**P>|z|**	**[95% Conf.**	**Interval]**
Long	.0729965	.1932428	0.38	0.706	-.3057525	.4517455
Personalized	.136812	.1946376	0.70	0.482	-.2446706	.5182947
Positive	-.0391277	.1935103	-0.20	0.840	-.4184008	.3401455
Negative	.1376376	.1943177	0.71	0.479	-.2432182	.5184933
Gain	.0933604	.1936109	0.48	0.630	-.28611	.4728307
Loss	-.039291	.1929705	-0.20	0.839	-.4175063	.3389244
Female	.1148152	.1934244	0.59	0.553	-.2642896	.4939201
Male	-.139057	.1918896	-0.72	0.469	-.5151537	.2370397
Visual id	.0009505	.1937703	0.00	0.996	-.3788322	.3807333
Number of obs = 600		LR chi2(9) = 4.04				
Prob > chi2 = 0.9088		Log likelihood = -848.62809			Pseudo R2 = 0.0024	

Table 41 shows that the male anthropomorphic character has a positive effect on the item *knowledge_public* compared to the control group.

Table 41: Ordered probit regression to test the effect of the treatments on *knowledge_public*

Treatments	Coef.	Std.Err	z	P>|z|	[95% Conf.	Interval]
Long	.113067	.2105675	0.54	0.591	-.2996378	.5257718
Personalized	.1434545	.2131517	0.67	0.501	-.2743152	.5612242
Positive	.1788493	.2142194	0.83	0.404	-.2410129	.5987116
Negative	.1892171	.2134107	0.89	0.375	-.2290602	.6074944
Gain	.1002841	.2122727	0.47	0.637	-.3157627	.5163309
Loss	.2612154	.2146086	1.22	0.224	-.1594098	.6818406
Female	.3426481	.2180533	1.57	0.116	-.0847285	.7700246
Male	.4447218	.2212366	2.01	**0.044**	.0111061	.8783375
Visual id	.251784	.2144747	1.17	0.240	-.1685787	.6721467
Number of obs = 600		LR chi2(9) = 6.04				
Prob > chi2 = 0.7358		Log likelihood = -613.26132			Pseudo R2 =	0.0049

From this point, the tables provide the results of testing knowledge items with their related behavioural outcomes. It means that, for example, *knowledge_safe* (knowing that connecting to a trusted connection can help you prevent from being attacked while online), should have a positive effect on the behavioural outcome *secure connection* (choosing a secure connection over an unsecured one).

Table 42 shows the effect of *knowledge_safe* on the behavioural outcome *secure connection.* There is a positive significant effect of knowing that connecting to a trusted connection may help prevent from being attacked while online, and performing the behaviour of choosing a trusted connection.

Table 42: Anova to test the effect of *knowledge* on *secure connection*

Source	Partial SS	Df	MS	F	Prob>F
Model	.29383881	4	.0734597	3.27	0.0115
Knowledge_safe	.29383881	4	.0734597	3.27	**0.0115**
Residual	13.379495	595	.02248655		
Total	13.673333	599	.02282693		
Number of obs = 600		R-squared = 0.0215			
Root MSE = .149955		Adj R-squared = 0.0149			

Table 43 test the effect of *knowledge_pswd1* on the behavioural outcome *password strength.* The results show no effect of knowledge on the dependent variable.

Table 43: Anova to test the effect of *knowledge_pswd1* on *password strength*

Source	Partial SS	Df	MS	F	Prob>F
Model	8.3198552	4	2.0799638	2.03	0.0881
Knowledge_pswd1	8.3198552	4	2.0799638	2.03	0.0881
Residual	608.37348	595	1.0224764		
Total	616.69333	599	1.0224764		
Number of obs = 600		R-squared = 0.0135			
Root MSE = 1.01118		Adj R-squared = 0.0069			

Table 44 test the effect of *knowledge_pswd2* on the behavioural outcome *password strength.* The results show no effect of knowledge on the dependent variable.

Table 44: Anova to test the effect of *knowledge_pswd2* on *password strength*

Source	Partial SS	Df	MS	F	Prob>F
Model	.61449469	4	.15362367	0.15	0.9637
Knowledge_pswd2	.61449469	4	.15362367	0.15	0.9637
Residual	616.07884	595	1.0354266		
Total	616.6933	599	1.0295381		
Number of obs = 600		R-squared = 0.0010			
Root MSE = 1.01756		Adj R-squared = -0.0057			

Table 45 tests the effect of *knowledge_pswd3* on the behavioural outcome *password strength.* The results show no effect of knowledge on the dependent variable.

Table 45: Anova to test the effect of *knowledge_pswd3* on *password strength*

Source	Partial SS	Df	MS	F	Prob>F
Model	1.5597442	4	.38993604	0.38	0.8250
Knowledge_pswd3	1.5597442	4	.38993604	0.38	0.8250
Residual	615.13359	595	1.033838		
Total	616.69333	599	1.0295381		
Number of obs = 600		R-squared = 0.0025			
Root MSE = 1.01678		Adj R-squared = -0.0042			

Table 46 test the effect of *knowledge_signup* on the behavioural outcome *sign-up info.* The results show no effect of knowledge on the dependent variable.

Table 46: Anova to test the effect of *knowledge_signup* on *sign-up info*

Source	Partial SS	Df	MS	F	Prob>F
Model	81.082451	4	20.270613	2.22	0.0656
Knowledge_signup	81.082451	4	20.270613	2.22	0.0656
Residual	5434.5025	595	9.1336177		
Total	5515.585	599	9.2079883		
Number of obs = 600		R-squared = 0.0147			
Root MSE = 3.02219		Adj R-squared = 0.0081			

Table 47 test the effect of *knowledge_trust* on the behavioural outcome *trusted vendor.* There is a positive significant effect of knowing that connecting to a trusted site may help prevent from being attacked while online, and performing the behaviour of choosing a trusted provider.

Table 47: Anova to test the effect of *knowledge_trust* on *trusted vendor*

Source	Partial SS	Df	MS	F	Prob>F
Model	2.9258779	4	.73146948	3.37	0.0096
Knowledge_trust	2.9258779	4	.73146948	3.37	**0.0096**
Residual	129.04746	595	.21688648		
Total	131.97333	599	.22032276		
Number of obs = 600		R-squared = 0.0022			
Root MSE = .465711		Adj R-squared = 0.0156			

Table 48 test the effect of *knowledge_logout* on the behavioural outcome *log-out.* The results show no effect of knowledge on the dependent variable.

Table 48: Anova to test the effect of knowledge_logout on *log-out*

Source	Partial SS	Df	MS	F	Prob>F
Model	1.2590501	4	.31476252	1.68	0.1522
Knowledge_logout	1.2590501	4	.31476252	1.68	0.1522
Residual	111.24095	595	.18695958		
Total	112.5	599	.18781302		

Number of obs = 600 R-squared = 0.0112
Root MSE = .432388 Adj R-squared = 0.0045

How to obtain EU publications

Our publications are available from EU Bookshop (http://bookshop.europa.eu),
where you can place an order with the sales agent of your choice.

The Publications Office has a worldwide network of sales agents.
You can obtain their contact details by sending a fax to (352) 29 29-42758.

LF-NA-28154-EN-N

JRC Mission

As the science and knowledge service of the European Commission, the Joint Research Centre's mission is to support EU policies with independent evidence throughout the whole policy cycle.

EU Science Hub
ec.europa.eu/jrc

@EU_ScienceHub

EU Science Hub - Joint Research Centre

Joint Research Centre

EU Science Hub

Publications Office

doi:10.2791/597150

ISBN 978-92-79-62758-3