NOTE. This is the **Accepted Author Manuscrip**t version. IT contains the final revised version of the paper, but no editoral changes, pagination or journal artwork. When you are citing it, please use the following citation information (here formatted as APA 6th):

Modic, D., & Anderson, R. J. (2014). *Reading This May Harm Your Computer: The Psychology of Malware Warnings*. Computers in Human Behavior, 41, 71-79. doi: 10.1016/j.chb.2014.09.014

Reading This May Harm Your Computer: The Psychology of Malware Warnings

David Modic[a]

Ross Anderson[b]

[a,b] University of Cambridge Computer Laboratory

JJ Thomson Avenue, Cambridge CB3 0FD, England

[a]email address: david.modic@cl.cam.ac.uk
(Corresponding author)
Tel: +44 1223 767014
Fax: +44 1223 334678

[b]email address: ross.anderson@cl.cam.ac.uk

Abstract

Internet users face large numbers of security warnings, which they mostly ignore. To improve risk communication, warnings must be fewer but better. We report an experiment on whether compliance can be increased by using some of the social-psychological techniques the scammers themselves use, namely appeal to authority, social compliance, concrete threats and vague threats. We also investigated whether users turned off browser malware warnings (or would have, had they known how).

Keywords

malware, persuasion, human computer interaction, psychology

1. Introduction

In life, as on the Internet, most of us are satisficers – we tend to favour actions and make decisions that are good enough, rather than optimal (Simon, 1956). As an energy-saving technique, this has benefits, but also drawbacks. When it comes to protecting oneself online, Akhawe and Felt (2013) and Herley (2010) have shown that Internet users work hard to ignore warnings and security notices. Existing theories and empirical work in criminology suggest this might be a problem. Situational crime prevention shows that offenders are more likely to take advantage of an environment that appears target-rich (cf. Felson & Clarke, 1998), while routine activity theory (RAT; Cohen & Felson, 1979) analyses crime incidence in terms of a motivated offender, a suitable target and an opportunity. However, there is comparatively little research on the causal link between ignoring warnings and being defrauded. One plausible explanation is that those who ignore the warnings might believe

themselves to be less vulnerable because they might have less money to lose or are confident in their ability to resist scams. In reality, lack of funds does not pose a hurdle for determined scammers, who have been known to push prospective victims into taking loans (e.g. in investment scams; Stevenson, 2000) or entangle them in money laundering schemes (Zuckoff, 2005). Overconfidence in one's ability to resist fraud has also been shown to increase the likelihood of being scammed (Camerer & Lovallo, 1999; Fischer, Lea, & Evans, 2013).

While computer users are more likely to follow an inconvenient procedure if they are explicitly told it is for security purposes (Serge Egelman, et al., 2010), the daily exposure to an overwhelming amount of warnings remains an issue. This makes it hard for users to sort the real threats from the many trivial ones and the even greater number of false alarms (Bravo-Lillo, et al., 2013). Users are willing to expend only a certain amount of effort and time on security concerns: that is, their *compliance budget* (Beautement, Sasse, & Wonham, 2008) is a limited resource. In brief, users would prefer to ignore warnings, but if that is hard enough they will comply with some of them, up to a point.

Thus there is a need for fewer but more effective of malware warnings, particularly in browsers. Earlier research tended to focus on the presentation of warnings; for example, passive warnings (that require no user action) tend to be almost universally ignored. S. Egelman, Cranor, and Hong (2008) found that active warnings helped deter 79% of their participants from visiting a potentially harmful website. Later research has moved towards the positioning of the dialogues, the amount of text, the length of the message and the amount of technical detail (Bauer, Bravo-Lillo, Cranor, & Fragkaki, 2013). Another recent approach has been to manipulate the content of security warnings (e.g. malware warnings;Serge Egelman & Schechter, 2013; and SSL warnings; Sunshine, Egelman, Almuhimedi, Atri, & Cranor,

2009). The wording in warnings in such studies generally appears to be based on trial and error rather than on established psychological theories of communication or persuasion. In the present paper, we based our warnings on some of the social psychological factors that have been shown to be effective when used by scammers (Modic, 2013; Modic & Lea, 2013). Those factors which play a role in increasing potential victims' compliance with fraudulent requests, will also prove effective in warnings.

1.1 Social psychological factors informing compliance with warnings

Previous research in the social psychology of persuasion (cf. Cialdini, 2001) has uncovered several factors that can influence our decision making abilities and increase compliance. Fischer, Lea, and Evans (2009) have shown in their report for UK Office of Fair Trade that social psychological mechanisms of persuasion such as influence of Authority and Social influence increase compliance with postal fraud. In addition Modic and Lea (2013) have developed a scale of Susceptibility to Persuasion that has been validated on victims of Internet fraud and has shown that same mechanisms we are using in this research, when used by scammers, are effective in reducing resistance of potential victims. The mechanisms effectively used by scammers on potential victims, would be likely just as effective when used by browser designers to increase scam resistance of potential victims.

Influence of Authority. Individuals are likely to respond to requests from authority figures across a range of cognate domains. For example, Titus and Dover (2001) show scammers using authority to elicit compliance with building inspector frauds and other scams. In postal fraud, Fischer, et al. (2013) showed that potential victims were more likely to comply with requests from scammers with ostensible formal authority. Tyler and Degoey (1995) found that individuals are more willing to show self-restraint in social dilemmas when they perceive the requesters to be fair and honest. Trust in authority figures increases their

influence. Murphy (2004) has shown that individuals are more likely to pay taxes when they trust the tax authorities. We thus hypothesize (H1) that warnings will be more effective when potential victims believe that they come from a trusted authority.

Social influence. Human susceptibility to group pressure or social influence is well supported empirically, from early line experiments by Asch (1956) to newer work: for example, Markus and Kitayama (1991) showed that individuals in different cultures construct their self-worth through comparison with other in-group members. Criminologists have found that individuals are more likely to comply with formal norms if they believe other members of their community also comply with them, while on the other hand visible disorder is a self-reinforcing cue for criminal activity (Kahan, 1997). Consumers susceptible to social influence may buy products a seller favours even if their preferences are different (Bearden, Netemeyer, & Teel, 1989). A malware warning exposing a potential threat to an individual's in-group might thus work across cultural contexts. We hypothesize that (H2) a warning constructed to solicit compliance with in-group norms would increase the likelihood of visiting a potentially harmful site even against the individuals' initial wishes.

Risk preferences. Individuals in general tend to act irrationally under risky conditions (Kahneman & Tversky, 1979; Munro, 2009; Rubinstein, 1997). They are willing to forgo privacy concerns to feel safer (Jagatic, Johnson, Jakobsson, & Menczer, 2007). And a study by Titus and Dover (2001) showed that repeated communication that varied the perceived risk of an unfavourable outcome increased compliance by potential victims. We hypothesize (H3) that straight talk would be effective in warnings; a concrete threat with clearly describes possible negative outcomes should increase compliance compared to a vague one.

1.2 The decision to keep malware warnings turned on

There is an underlying assumption in security-warnings research that most users will keep the warning mechanisms on their default setting (i.e. turned on). There is tangential empirical support for this claim. Spool (2011) has shown that nine out of ten individuals keep all the default settings in a popular text-processing package. The preference for things to stay the same (the status quo bias; see Ert & Erev, 2008; Kahneman, Knetsch, & Thaler, 1991) has strong support in other domains, from voters' propensity to keep existing political parties in power (Jost, Banaji, & Nosek, 2004) to consumer decision making (Anderson, 2003). Nevertheless, we wanted to test the status quo bias empirically for security warnings in order to determine how many individuals turn them off and why.

Although only a minority of users may turn off malware warnings, there are various possible reasons for departure from it. (a) Some individuals prefer to make their own decisions; Lee and See (2004) report that individuals are reluctant to trust automated systems, when they have insufficient information about their operation. (b) Others might want to turn the warnings off because they ignore them anyway and just click through them. (c) Some will turn warnings off because they impact their productivity and are a waste of time. As Herley (2009) shows, this sentiment is realistic to a point – only a small percentage of Internet users suffer a setback from ignoring security advice; and skilled users consider many warnings pointless (as a Google manager said to us: 'Surely I am invulnerable to phishing?'). (d) Some individuals might not understand the warnings and would thus prefer to not see them. (e) There might be too many false positives. Krol, Moroz, and Sasse (2012) show this to be an important issue in user decision-making. And finally, (f) many non-Windows users might feel that malware warnings are only relevant to Microsoft Windows users.

We therefore want to understand the extent to which some individuals depart from the default option. We hypothesize (H4) that the main reason for turning off malware warnings is the wish to remain productive and avoid being derailed by security notices. Furthermore, we hypothesize that (H5) the reasons for turning the malware warnings off will differ between the participants who kept the warnings on and those who turned them off (or expressed a wish to do so).

1.3 Aims

The present study aims to show the following: (a) Confirm the status-quo bas when it comes to malware warnings and analyse the self-reported reasons of why it is violated; and (b) show which textual treatment of browser malware warnings is effective in eliciting compliance.

2. Method

2.1 Participants

Our respondents for this study were recruited via Amazon Mechanical Turk (mTurk). In total, 583 mTurkers responded, and were distributed evenly across five conditions. In several cases same respondents participated in more than one condition. These duplicates were omitted from further analysis. In addition we removed incomplete cases, leaving us with 496 valid responses. The respondents were paid $0.70 on average per finished survey. In the measured group, age was normally distributed with a peak between 26 and 30 years of age. Gender was self-reported as 207 (42%) female and 281 (57%) male (8 respondents refusing to answer). Most of the respondents were United States residents. More demographics are given in the Results Section.

2.2 Experimental design

2.2.1 Dependent variables.

There were three dependent variables in the present experiment:

Malware (strict) was a two outcome variable, where respondents reported (1) turning anti-malware warnings in browsers off; or (2) keeping them turned on.

Malware (relaxed) was a two outcome variable, where the respondents reported whether they (1) turned the anti-malware warnings off or that they would like to turn them off if they were able to; or (2) kept the anti-malware warnings on.

Visit was a Likert 1-7 type item asking the respondents to mark how likely they were to follow a link to a potentially harmful website after they had read a warning message.

2.2.2 Independent variables

There were eleven independent psychological variables in this experiment, one manipulated experimentally, the others measured correlationally. Demographic data, browser usage patterns and social network membership data were also collected.

Warning type was a between-groups experimental variable with five levels (control – same text as in Google Chrome browser as of June 2013; authority; social influence; concrete threat; and vague threat. cf. Table 1 for details).

Respondents were additionally asked why individuals would be likely to turn off anti-malware warnings (if they had kept them on); or what their rationale for turning the warnings off was (if they had turned them off). These items were worded in the same manner, the only change being the actor of the sentence (i.e. “I just ignore these kinds of warnings” vs. “They

just ignore these kinds of warnings"). The items in this group are contained in Table 2. An open text item, titled "Other" was also included in the experiment, allowing us to catch any reasons we did not specify outright, but none of the respondents mentioned any other possible reasons.

In addition, we asked a series of questions about the perception of trust in various groups. Again, these were all Likert type (1-7) items. For more details, see Table 3.

Table 1
Manipulated Warning Text Across five Conditions

Condition	Text
Control	Control text has been taken from Google Chrome anti-malware warning as of June 2013.[a]
Authority	The site you were about to visit has been reported and confirmed by our security team to contain malware. We strongly encourage you to avoid visiting this page.
Social Influence	The site you were about to visit contains software that can damage your computer. The scammers operating this site have been known to operate on individuals from your local area. Some of your friends might have already been scammed. Please, do not continue to this site.
Concrete Threat	The site you are about to visit has been confirmed to contain software that poses a significant risk to you, with no tangible benefit. It would try to infect your computer with malware designed to steal your bank account and credit card details in order to defraud you.
Vague Threats	We have blocked your access to this page. It is possible that it might contain software that might harm your computer. Please close this tab and continue elsewhere.

Note. [a] Text: 'Warning - visiting this web site may harm your computer! Suggestions: • Return to the previous page and pick another result. • Try another search to find what you're looking for. Or you can continue to [%site%] at your own risk. For detailed information about the problems we found, visit Google's Safe Browsing diagnostic page for this site. For more information about how to protect yourself from harmful software online, you can visit stopBadware.org. If you are the owner of this web site, you can request a review of your site using Google's Webmaster Tools. More information about the review process is available in Google's Webmaster Help Center. Advisory provided by Google.
Instructions: "You are surfing the net, looking to secure cheap holiday accommodation for yourself and some people close to you. You search for the sites offering budget tickets and hotel reservations. You follow a link to a certain page you have never visited before. You click on the link and get a screen similar to the one below."

Table 2
Reasons for turning Off Browser Warnings

Item	Statement
Make own decision	I want to decide what is good for me, not the computer
Ignores warnings	I generally never read the warnings, I just click them away
Hassle	I don't like the hassle of having to get past these particular warnings
Not understand	I prefer to ignore unintelligible messages about things I don't understand
False positives	It keeps warning me about sites that I know and in my opinion pose no threat
Not Windows	These warnings do not apply to me as I am not using a Windows machine

Note. Responses were recorded as strength of agreement on a 1 -7 Likert type scale.

Table 3
Trust Items

Trusts Developer	The team who designed my [%BROWSER%] has my best interests at heart
Trust Company	I trust the company that designed [%BROWSER%]
Not Trust Authority	I would never trust a huge corporation to decide what is good for me
Trust Friends	I think it is safe to ignore the warning if a good friend tells me the site is safe
Trusts Facebook Friends	I think it is safe to ignore this warning if my friends on facebook tell me the site is safe

Note. [%BROWSER%] was replaced at runtime with the name of the browser respondents indicated that they used the most.

Finally, we asked the respondents to indicate what kind of information would make anti-malware warnings more salient for them. They had to rank the items in this group on a Likert-type scale, according to importance (cf. Table 4).

Table 4
Items on Improving the Effectiveness of Anti-malware Warnings

Certainty	Level of certainty that the site you are about to visit is a fraudulent site (e.g. 90% certain).
Mechanics	How a particular scam works
Amount Lost (Typical)	The amount of money that is typically lost to this scheme.
Amount Lost	The amounts of money lost to this kind of scheme on average [per scam].
Affected	How many people are generally affected in this kind of scheme.
Local	How many people in your local area are affected on average by this kind of fraud.

Note. Instructions were: Which information should be contained in these warnings, to make them more effective?

2.3 Design

To control for order effects the items in each section of the survey were randomised. The survey was delivered online in a form of an mTurk human intelligence task (HIT). All participants answered the exploratory and demographic questions at beginning of the survey. The survey was available online for 30 days, and most of the participants completed it within two hours of starting it.

Two analyses were run in addition to supplementary tests. To test for the rationale of turning anti-malware warnings off, a series of logistic regressions were run with Malware (strict) and Malware (relaxed) as a dependent variable (DV) and demographic factors, browser usage, social networking membership, reasons for turning malware warnings off; and trust questions as possible explanatory variables.

In the second analysis a series of multiple regressions were run with click through as the DV and demographics, group, browser usage, social networks membership, trust items

and expectations items as the IV.

2.4 Procedure

The survey was delivered online, and consisted of five sequential parts:

1. Introduction to the experiment, with a brief explanation of the structure and our reasoning for using it; assurance of anonymity; and a request for permission to use the data in the analysis.
2. Demographics, browser usage, social networking membership, familiarity with anti-malware mechanisms; and the rationale for keeping malware warnings on (or off).
3. Manipulation task; the questions about clicking through to the site and trust items.
4. Items on improving efficiency of malware warnings.
5. Demand characteristics question and debriefing.

3. Results

3.1 initial analysis

Data were initially screened for duplicates. 63 records were removed several respondents with the same mTurker ID had already answered the questionnaire (mTurker ID's were then removed from further analysis, preserving anonymity). Only the first response from each unique ID was retained, leaving us with a sample size of 520.

IT proficiency was distributed moderately leptokurtically, but without skewness, with 415 (80%) respondents claiming to be very proficient in IT (mean = 4.32 out of 6, SD = 0.88). Educational level was normally distributed with 240 (46%) respondents holding a bachelor's degree. As for web browser usage, 51% of the tested population named Google Chrome as their primary browser, followed by Firefox (37%) and Internet Explorer (7%). All

other listed browsers (Safari, Opera, Chromium) were reported as used by less than 1% of respondents. None of the respondents reported using other browsers as their primary one. In social networks, 439 (84%) reported to be Facebook members, followed by Twitter (51%), Google Plus (46%), LinkedIn (42%), Pinterest (23%), Tumblr (14%), Path (1%) and Diaspora (< 1.0%). No respondents reported membership of any other social network.

3.2 Malware warnings

Out of valid responses in this part of the survey (n = 383), 17 (3%) respondents indicated that they turned the malware warnings off (the strict DV condition) and 51 (10%) indicated that they either turned it off, or would if they knew how (the relaxed one).

Table 5
Reasons for turning Off Browser Warnings

	Warnings ON (n = 323)		Warnings OFF (Strict) (n = 16)		Warnings OFF (Rel.) (n = 49)	
Item	Mean	S.D.	Mean	S.D.	Mean	S.D.
Make own decision	4.59	1.70	5.19	2.07	4.78	1.82
Ignores warnings	5.46	1.46	2.75	2.11	3.48	2.07
Hassle	5.41	1.48	4.71	2.23	4.41	1.82
Not understand	4.97	1.72	3.53	2.48	3.73	2.02
False positives	5.60	1.42	5.47	1.97	5.27	1.69
Not Windows	3.46	1.78	2.24	1.92	3.08	2.04

Note. Responses were recorded as strength of agreement on a 1-7 Likert type scale (1 indicates lowest level of agreement, 7 highest level of agreement).

Descriptive analysis shows that across all groups, the leading reason for individuals to turn the warnings off is a high rate of false positives. Further analysis will clarify this point later.

3.3 Turning off malware warnings

In order to predict which items influence a decision to turn off malware warnings, three logistic regressions were run. We evaluated the bivariate Spearman rho correlations

between the subscales of the IV's and performed model diagnostics. There were four significant correlations above .350 in the present sample. Ignores warnings was significantly positively correlated with hassle ($r_{387} = .447$, $p < .001$) and not understand ($r_{387} = .409$, $p < .001$). Trusting the company that created the respondents primary browser was significantly positively correlated with trusting the team that developed it ($r_{387} = .630$, $p < .001$). And trusting a friend in the concrete world was significantly positively correlated with trusting a friend on Facebook ($r_{387} = .703$, $p < .001$). None of the variables were removed from further analysis, but additional collinearity diagnostics were run on the remaining variables. There was a high condition index in the 28th dimension of the model (Trust in Facebook friends; 58.218), but the variance proportion did not rise above .12 across any of the other variables, confirming that we could proceed with the regression (Tabachnick & Fidell, 2005, pp. 90-91). The first two regression models are reported in Table 6.

Overall goodness of fit for Model 1 in the first analysis was 93.5%, showing that we could successfully predict when individuals would turn anti-malware warnings off in most cases (cf. Table 7). There was 2% difference between the goodness of fit of Model 1 and the null hypothesis model, with the latter incorrectly categorizing 100% of the warnings-off cases. The regression was statistically significant (Model $\chi^2 = 67.55$, $p < .001$) and had good predictive strength (Nagelkerke pseudo $R^2 = .59$). Turning off malware warnings was significantly predicted by IT proficiency (the more familiar the user is with IT, the more likely they are to switch the warnings off), use of some social networks (i.e. Path), the habit of ignoring warnings (discussed later) and mistrust in authority. A number of statistically significant predictors at $p < .1$ emerged – gender, wanting to decide on their own, not clearly understanding the warnings, not using Microsoft Windows and trusting Facebook friends.

Table 6
Logistic Regression Models for Anti Malware Notifications

	Model 1: Strict (All Variables) (n = 354)				Model 2: Relaxed (All Variables) (n = 354)			
	b	*exp (b)*	S.E.	Wald	*b*	*exp(b)*	S.E.	Wald
Age	0.22	1.25	0.17	1.74	0.22	1.25	0.17	1.75
IT Proficiency	0.65	1.91	0.24	7.06**	0.65	1.91	0.24	7.07**
Gender	0.96	2.60	0.50	3.63*	0.96	2.61	0.50	3.67*
Level of Education	-0.21	0.81	0.27	0.61	-0.21	0.81	0.27	0.61
Use Internet Explorer	0.64	1.89	1.05	0.37	0.64	1.89	1.05	0.37
Use Safari	-1.26	0.28	1.13	1.24	-1.26	0.28	1.13	1.24
Use FireFox	0.14	1.15	0.48	0.09	0.14	1.15	0.48	0.09
Use Facebook	0.14	1.15	0.84	0.03	0.14	1.15	0.84	0.03
Use LinkedIn	0.15	1.16	0.50	0.09	0.15	1.16	0.50	0.09
Use Google+	0.21	1.24	0.49	0.19	0.22	1.24	0.49	0.19
Use Twitter	0.20	1.22	0.50	0.15	0.20	1.22	0.50	0.15
Use Path	-3.69	0.02	1.56	5.59**	-3.69	0.02	1.56	5.6**
Use Pinterest	-0.52	0.60	0.57	0.82	-0.51	0.60	0.57	0.81
Use Diaspora	0.43	1.54	1.82	0.06	0.43	1.54	1.82	0.06
Use Tumbler	-0.05	0.95	0.83	0	-0.05	0.95	0.83	0
Make own decision	-0.26	0.77	0.14	3.46*	-0.26	0.77	0.14	3.45*
Ignores warnings	0.68	1.98	0.14	25.61***	0.68	1.98	0.14	25.73***
Hassle	0.23	1.26	0.15	2.4	0.24	1.27	0.15	2.41
Not understand	0.26	1.30	0.14	3.36*	0.26	1.29	0.14	3.34*
False positives	0.01	1.01	0.16	0.01	0.01	1.01	0.16	0.01
Not Windows	0.25	1.29	0.15	3.09*	0.25	1.29	0.15	3.09*
Trusts developer	-0.03	0.97	0.20	0.03	-0.03	0.97	0.20	0.03
Trust Company	0.06	1.06	0.21	0.07	0.06	1.06	0.21	0.08
Not Trust Authority	-0.27	0.76	0.13	4.11**	-0.27	0.76	0.13	4.1**
Trust Friends	-0.12	0.89	0.17	0.47	-0.12	0.89	0.17	0.47
Trusts Facebook Friends	-0.32	0.73	0.17	3.36*	-0.32	0.73	0.17	3.37*
Constant	-5.32	0.00	2.58	4.26**	-5.34	0.00	2.58	4.28**
Model χ^2 =				67.55***				107.11***
df				5				26
Nagelkerke R^2 =				.59				.49

Note. * p < 0.1; ** p < 0.05; *** p < 0.01

Table 7
Goodness of Fit for Logistic Regression (Model 1) - Strict Interpretation (n=354)

Observed	Predicted		
	Turned Off	Kept warnings	Correct [%]
Turned Off	13	2	86.7
Kept Warnings	21	318	93.8
Overall [%]			93.5

Note. The cut-off value was set at .9 (as it provided the optimal balance).

Overall goodness of fit for Model 2 in the first analysis was 82.8%, showing that we could successfully predict which regressors have an impact in the decision to turn off anti-malware warnings or influence the wish to do so (cf. Table 8). There was 4% difference between the goodness of fit of Model 1 and the null hypothesis model. Regression in Model 2 was also statistically significant (Model χ^2= 107.11, $p < .001$), with moderate predictive strength (Nagelkerke pseudo $R^2 = .49$). Turning off malware warnings, when this action is construed more broadly was significantly predicted by the same regressors as in Model 1.

Table 8
Goodness of Fit for Logistic Regression (Model 2) - Relaxed Interpretation (n=354)

Observed	Predicted		
	Turned Off	Kept warnings	Correct [%]
Turned Off	38	7	84.4
Kept Warnings	54	255	82.5
Overall [%]			82.8

Note. The cut-off value was set at .87 (as it provided the optimal balance).

The two models (i.e. strict and relaxed) are almost identical when taking into account significant regressors, their odds ratios and their Wald χ^2 values. This allows us to use the relaxed model for the next step.

The third logistic regression was run, taking into account only the regressors that were salient in the first analysis. The decision to turn off malware warnings (relaxed) was used as the DV. The model diagnostics were run in the initial analysis. The results of the analysis are reported in Table 9.

Table 9
Logistic Regression Models for Anti Malware Notifications (Relaxed Model)

	Model 1: Relaxed (Selected Variables) (n = 365)			
	b	*exp (b)*	S.E.	Wald
Age	0.24	1.27	0.16	2.31
IT Proficiency	0.64	1.90	0.22	8.83**
Gender	1.07	2.91	0.44	5.77**
Use Path	-4.07	0.02	1.37	8.85**
Make Own Decision	-0.26	0.77	0.13	4.07**
Ignores warnings	0.66	1.93	0.13	25.67***
Hassle	0.20	1.22	0.14	2.11
Not Understand	0.27	1.31	0.13	4.31**
Not Using Windows	0.22	1.24	0.13	2.81*
Does not trust any authority	-0.28	0.75	0.13	4.95**
Trusts Facebook friends	-0.38	0.68	0.12	9.46**
Constant	-5.62	0.00	1.78	10.02**
Model χ^2 =				103.57***
df				11
Nagelkerke R^2 =				.47

Note. * p < 0.1; ** p < 0.05; *** p < 0.01

Table 10
Goodness of Fit for Logistic Regression (Model 1) - Relaxed Interpretation (n=365)

Observed	Predicted		
	Turned Off	Kept warnings	Correct [%]
Turned Off	37	8	82.2
Kept Warnings	50	270	84.4
Overall [%]			84.1

Note. The cut-off value was set at .85 (as it provided the optimal balance).

Overall goodness of fit for Model 1 in the second analysis was 84.1%, showing that we could successfully predict when individuals would turn anti-malware warnings off in approximately 8 out of every 10 cases (cf. Table 10). There was a 72% increase of predictive strength from the null hypothesis model. The regression was statistically significant (Model χ^2= 103.57, $p < .001$) and had moderate predictive strength (Nagelkerke pseudo $R^2 = .47$). Nine out of 11 predictors in the analysis were statistically significant, the strongest being ignores warnings (Wald $\chi^2 = 25.67$; $p < .001$). Its odds ratio indicates that for every unit of increasing level of agreement with the wish to ignore malware warnings, individuals are approximately twice as likely to keep the warnings on.

3.4. Clicking through to a fraudulent web-site

Respondents across groups were not very likely to follow the link to the page containing malware, regardless of condition with means (and standard deviations): control = 2.27 (1.62); authority = 1.85 (1.24); concrete threat = 1.91 (1.46); social influence = 2.31 (1.54); vague threats = 2.51 (1.72). These indicate that respondents in general are likely to heed malware warnings, regardless of what the warnings say. The data also show that use of authority and concrete threat has a greater effect effect compared with the default text.

Analysis showed that visit was not normally distributed (it was positively skewed; skewness = 1.285, S.E. = .104; with additional positive kurtosis; kurtosis = .624, S.E. = .104).

On a scale of 1 to 7 where 1 was extremely unlikely and 7 extremely likely, 81% of respondents scored 3 or less and 49% scored it as 1 (minimum). Only 1% of respondents scored visit as 7 (maximum). To test for the difference between the conditions a non-parametric independent samples (Kruskal-Wallis) test was performed that showed significant differences across the five conditions (at $p = .004$). A Mann-Whitney U test showed that the likelihood of visiting a fraudulent site was significantly ($p = .009$) different when comparing the control group against all other conditions combined. We have transformed visit using Box-Cox transformation (Box & Cox, 1964; Osborne, 2010) and thus lowered its skewness to 0.005, but when we ran multiple regression models, no substantial differences in the results were found across transformed and untransformed dependent variables.

In order to run multiple linear regression on small sample sizes, the DV has to be normally distributed, but with sample sizes of more than a 100 respondents the effects of skewness and kurtosis can be safely ignored (Tabachnick & Fidell, 2005, pp. 79-80). Furthermore, when data across groups have the same direction and approximate level of skewness and kurtosis (as in the present experiment), general linear model testing can be safely conducted (Kirk, 2013, p. 99). In addition general linear methods have proven to be robust when normality assumption is violated (Harwell, 2003; Lix, Keselman, & Keselman, 1996; Schmider, Ziegler, Danay, Beyer, & Bühner, 2010). For these reasons untransformed visit was used in the following analysis.

Multiple linear regression was employed to determine which factors influence the decision to visit a web page containing malware. Outliers at the 3SD level were removed as were incomplete responses. Homoscedasticity was examined via several scatterplots which indicated an adequate consistency of spread through the distributions. Collinearity diagnostics were run on the remaining data and there was a marginally high condition index in the 24th

dimension of the model (Amount Lost; 34.967), but the variance proportion did not rise above .5 across any of the other variable pairs, confirming that we could proceed with the regression (Tabachnick & Fidell, 2005, pp. 90-91).

The correlations amongst the IVs were examined. Trust in the team was positively correlated with trust in the company ($r_{491} = .626$, $p < .001$) and negatively correlated with the trust in authorities in general ($r_{491} = -.285$, $p < .001$). Trust in authority was furthermore negatively correlated with trust in the company ($r_{491} = -.315$, $p < .001$). This indicates that individuals who mistrust authority in general also do not trust companies or their employees. Those who would trust their real-life friends also trust their Facebook friends ($r_{491} = .646$, $p < .001$). Expectations of finding out how much money was lost in general and in the specific case were closely correlated ($r_{491} = .809$, $p < .001$), indicating that our items could be worded more distinctively in this case. Individuals who expected to know how many people were affected in their local area, also wanted to know how a particular scam works ($r_{491} = .297$, $p < .001$), amount lost (typical: $r_{491} = .515$, $p < .001$; and specific: $r_{491} = .530$, $p < .001$); and how many people in general are affected by this kind of scam ($r_{491} = .526$, $p < .001$). Individuals who expected to know how many people in general were affected by a certain type of fraud, would also like to be informed about how a scam works ($r_{491} = .312$, $p < .001$) and the amount of money lost (typical: $r_{491} = .550$, $p < .001$; and specific: $r_{491} = .607$, $p < .001$).

A hierarchical method was used for the entry of the predictor variables. The independent variables were entered in six blocks (demographics; dummy variables for the condition, with the control as the baseline variable; dummy variables for the primary browser with Google Chrome left out; social-network membership; trust items and expectations items). Missing or incomplete cases were removed listwise. Gradually, least significant predictors were removed from subsequent regressions, until only significant ones remained.

Beta weights and regression coefficients for the sequence of regressions are reported in Table 11, while model statistics are reported in Table 12.

The final regression analysis produced an R of .668, $R^2 = .446$ and an adjusted R^2 of .436 ($F_{1, 517} = 45.412$, $p < .001$) with ten significant predictors of the likelihood to visit a fraudulent site and observed power of .891.

Table 11

Regression Coeficients and Beta Weights of Variables Included in the Hiearchical Regression Analysis to the Likelihood of Clicking Through to a Fraudulent Site

		b	SE b	β	t
Step 1	(Constant)	2.96	0.53		5.57***
(n = 484)	Internet Proficiency	-0.20	0.06	-0.12	-3.21**
	Gender	0.11	0.11	0.04	1.02
	Age	-0.12	0.04	-0.12	-3.24**
	Authority Group	-0.31	0.17	-0.08	-1.80*
	Concrete Threat Group	-0.30	0.16	-0.08	-1.90*
	Social Influence Group	0.08	0.17	0.02	0.50
	Vague Threats Group	0.16	0.16	0.04	1.01
	Uses Firefox	0.24	0.11	0.08	2.13**
	Uses Chromium	0.61	0.39	0.06	1.56
	Google Plus user	-0.25	0.11	-0.08	-2.36**
	Safe to ignore (Facebook)	0.40	0.04	0.45	9.56***
	Safe to Ignore (friend)	0.12	0.04	0.14	3.03**
	Trust in the company	-0.09	0.04	-0.09	-2.52**
	Certainty that the site is malicious	-0.05	0.04	-0.05	-1.20
	Scam Mechanics	-0.01	0.04	-0.01	-0.17
	The amount of money lost - specific	0.04	0.05	0.05	0.86
	The amount of money lost - general	-0.02	0.05	-0.02	-0.35
	People affected - general	-0.03	0.04	-0.04	-0.86
	People affected - specific	-0.03	0.04	-0.03	-0.77
Step 2	(Constant)	3.07	0.45		6.75***
(n = 502)	Internet Proficiency	-0.18	0.06	-0.11	-3.13**
	Age	-0.12	0.04	-0.12	-3.31**
	Authority Group	-0.43	0.14	-0.11	-3.13**
	Concrete Threat Group	-0.39	0.13	-0.11	-3.10**
	Uses Firefox	0.62	0.39	0.06	1.60
	Uses Chromium	0.20	0.11	0.06	1.86*
	Google Plus user	-0.23	0.10	-0.08	-2.21**
	Safe to ignore (Facebook)	0.40	0.04	0.46	10.21***
	Safe to Ignore (friend)	0.12	0.04	0.14	3.21**
	Trust in the company	-0.09	0.04	-0.08	-2.46**
	Certainty that the site is malicious	-0.06	0.04	-0.05	-1.50
	The amount of money lost - specific	0.02	0.03	0.03	0.75
	People affected - general	-0.05	0.04	-0.06	-1.41
Step 3	(Constant)	3.12	0.42		7.37***
(n = 518)	Internet Proficiency	-0.18	0.06	-0.11	-3.21**
	Age	-0.11	0.04	-0.11	-3.16**
	Authority Group	-0.45	0.14	-0.11	-3.28**
	Concrete Threat Group	-0.39	0.13	-0.11	-3.11**
	Google Plus user	-0.23	0.10	-0.08	-2.24**
	Safe to ignore (Facebook)	0.41	0.04	0.47	10.68***
	Safe to Ignore (friend)	0.11	0.04	0.13	3.03**
	Trust in the company	-0.09	0.04	-0.08	-2.50**
	Certainty that the site is malicious	-0.08	0.04	-0.07	-2.13**

Note: * p < 0.1, ** p < 0.05, *** p < 0.01

Table 12

Model Statistics for the Hierarchical Regression Analysis to Predict the Likelihood of Clicking Through to a Fraudulent Site (n = 484)

	Variables entered	R^2	R_{adj}^2	F	ΔF
Step 1	Internet Proficiency, Gender, Age, Authority Group, Concrete Threat Group, Social Influence Group, Vague Threats Group, Uses Firefox, Uses Chromium, Google Plus user, Safe to ignore (Facebook), Safe to Ignore (friend), Trust in the company, Certainty that the site is malicious, Scam Mechanics, The amount of money lost - specific, The amount of money lost - general, People affected - general, People affected - specific	.46	.44	20.907***	9.284***
Step 2	Internet Proficiency, Age, Authority Group, Concrete Threat Group, Uses Firefox, Uses Chromium, Google Plus user, Safe to ignore (Facebook), Safe to Ignore (friend), Trust in the company, Certainty that the site is malicious, The amount of money lost - specific, People affected - general	.46	.44	31.416***	8.745***
Step 3	Proficiency, Age, Authority Group, Concrete Threat Group, Google Plus user, Safe to ignore (Facebook), Safe to Ignore (friend), Trust in the company, Certainty that the site is malicious	.45	.44	45.412***	4.7673***

Note: * $p < 0.1$, ** $p < 0.05$, *** $p < 0.001$

The two significant modifications to the wording of warnings were authority (β = -0.11, p = .001, d = 0.29) and concrete threat (β = -0.11, p = .002, d = 0.24). Respondents also indicated that they were more likely to click through if their friends (β = 0.13, p = .003, d = -0.59) or Facebook friends (β = 0.47, p < .001, d = -0.36) told them that it was safe to do so. Facebook friends thus appear to have more sway on the decision to click through. Respondents also indicated that they would be marginally less likely to visit a web page containing malware if they were told the degree of certainty of maliciousness of the site (β = -

0.08, p = .034, d = -2.49). This ties in with authority and concrete threats as significant predictors.

4. Discussion

4.1. Status quo bias and departures from it

In the present study, we aimed to uncover the extent of status quo bias when it comes to malware warnings (and the rationale for departing from it) and construct a more effective malware warning by uncovering preferences for what these browser warnings should contain. The experiment showed that more than nine out of every ten participants kept the malware warnings in browsers turned on. This is in line with expectations from other domains (e.g. Anderson, 2003; Kahneman, et al., 1991; Thaler & Sunstein, 2008), but it is still a pertinent empirical finding. Another one out of ten participants indicated that they wanted to turn the warnings off, but were unsure of how to accomplish that, perhaps indicating a lack of familiarity with their browser more than anything else.

Our analysis showed that the more familiar our respondents were with computers, the more likely they were to keep the malware warnings on. Risk assessment is possibly more accurate in the population familiar with various cyber threats. This result indicates that the ability for premeditation outweighs the need for convenience to some extent. This is in line with previous research, Bhatnagar, Misra, and Rao (2000) showed that online shopping was counterbalanced by convenience on one side and the perception or risk on the other. Female respondents were more likely to keep the warnings on although the gender distribution across models was similar. Risk perception is influenced by gender in general (Gustafson, 1998) and females are more likely to perceive online transactions as riskier than males (Garbarino & Strahilevitz, 2004).

Respondents who turned warnings off indicated that the strongest reason was that they ignore malware warnings anyway. Previous research has shown that computer users will usually try to ignore requests from their computers (Akhawe & Felt, 2013; Herley, 2010); ignoring malware warnings is an extension of that finding.

The inability to understand the warnings was another significant predictor of turning the malware warnings off. We might infer that the language in existing warnings is not as clear as it could be. A report by Bauer, et al. (2013) offers guidelines on the length and content of warnings. It is unclear whether it has been taken into account by browser developers. In any case, clear, concise and concrete language is needed for effective malware prevention.

The last significant predictor of turning the warnings off was the expressed need to make one's own decisions. Research by Triandis, et al. (1986) shows that individualism and self-reliance are culturally dependent. This might be mitigated by online environments, but even in mixed online culture samples the level of trust in computer mediated communication still depends on the individual level of self-reliance (Kim, 2008). Wu and Tsang (2008) have shown that the level of compliance is also dependent on the level of institutional trust. Thus the need for self-reliance and mistrust in corporations both have an effect on individuals' wish to decide the amount of risk they are exposed to.

The importance of the power of default has been well researched (cf. Thaler & Sunstein, 2008) in other domains, from medicine (Halpern, Ubel, & Asch, 2007), through privacy studies (Johnson, Bellman, & Lohse, 2002) to decision-making under uncertainty (Samuelson & Zeckhauser, 1988). It proves to be salient in this case too.

4.2 The likelihood of following through to a fraudulent site

Multiple regression has yielded moderate results. The strongest predictors of click-through resistance were warnings that clearly outlined in concrete terms the risk an individual would take if they clicked through or the use of authoritarian techniques based on soft power (Raven, Schwarzwald, & Koslowsky, 1998). The effect sizes were small, but significant. In connection with these predictors, our respondents also self-reported the most effective warnings to be those that would clearly define the extent of risk. In brief, when individuals have a clear idea of what is happening and how much they are exposing themselves, they prefer to avoid potentially risky situations.

Mariani and Zappalà (2006) has shown that online consumer behaviour is strongly impacted by risk perception and when we approach malware from the perspective that every fraudulent activity can be construed as an illegitimate marketing offer (Fischer, et al., 2013) it is unsurprising that risk preferences would also impact the decision to visit a potentially fraudulent site.

A strong predictor, alongside with concrete threats, was the influence of authority. Two conditions in the present experiment were concerned with authority, one employing predominantly soft power techniques (Koslowsky, Schwarzwald, & Ashuri, 2001; Raven, et al., 1998), that is - expert, referent and informational power; while the other (n.s.) condition employed harsh power techniques (i.e. coercion, threats, etc). In line with previous findings, soft power of authority has also proven to be more effective in case of malware deterrence.

Another strong predictor was trust in the in-group opinion, with Facebook friends carrying more authority than concrete ones. This ties in authority as a significant predictor since, perhaps, Facebook friends carry more informative power than regular ones.

The impact of persuasive techniques on the wording of malware warnings was confirmed. These effects were weak, but significant, telling us that they should be taken into account in constructing future malware warnings.

4.3 Conclusion

In order to increase the effectiveness of warnings the experiment we report on shows that: (a) warning text should include a clear and non-technical description of potential negative outcome; or (b) an informed direct warning given from a position of authority. Concrete warnings are much more effective than vague ones; soft powers of persuasion work much better than harsh ones; and social influence appears to be much less effective than it is fashionable to believe. In fact, the use of coercion (as opposed to persuasion) should be minimized as it is rather likely to be counterproductive.

Acknowledgements

The first author was funded by Google and by the Engineering and Physical Sciences Research Council (EPSRC), United Kingdom, both of whom we wish to thank for supporting this research.

Bibliography

Akhawe, D., & Felt, A.P. (2013). Alice in Warningland: A Large-Scale Field Study of Browser Security Warning Effectiveness. In S. King (Ed.), *USENIX Security Symposium 2013*. Washington, D.C.: USENIX.

Anderson, C.J. (2003). The psychology of doing nothing: Forms of decision avoidance result from reason and emotion. *Psychological Bulletin,* 129(1), 139-167.

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), 1-70.

Bauer, L., Bravo-Lillo, C., Cranor, L., & Fragkaki, E. (2013). Warning Design Guidelines. In. Pittsburgh, PA: Carnegie Mellon University.

Bearden, W.O., Netemeyer, R.G., & Teel, J.E. (1989). Measurement of Consumer Susceptibility to Interpersonal Influence. *Journal of Consumer Research,* 15(4), 473-481.

Beautement, A., Sasse, A.M., & Wonham, M. (2008). The compliance budget: managing security behaviour in organisations. In A. Keromytis & A. Somayaji (Eds.), *NSPW '08 Proceedings of the 2008 workshop on New security paradigms* Lake Tahoe, California: ACM.

Bhatnagar, A., Misra, S., & Rao, H.R. (2000). On risk, convenience, and Internet shopping behavior - Why some consumers are online shoppers while others are not. *Communications of the Acm,* 43(11), 98-105.

Box, G.E.P., & Cox, D.R. (1964). An Analysis of Transformations. *Journal of the Royal Statistical Society. Series B (Methodological),* 26(2), 211-252.

Bravo-Lillo, C., Cranor, L., Downs, J., Komanduri, S., Reeder, R., Schechter, S., & Sleeper, M. (2013). Your Attention Please: Designing security-decision UIs to make genuine risks harder to ignore. In L. Bauer & K. Beznosov (Eds.), *The ninth Symposium on Usable Privacy and Security (SOUPS)* (pp. 18). Newcastle, UK: ACM SIGCHI.

Camerer, C., & Lovallo, D. (1999). Overconfidence and Excess Entry: An Experimental Approach. *The American Economic Review,* 89(1), 306-318.

Cialdini, R.B. (2001). *Influence : science and practice* (4th ed.). Boston, MA ; London: Allyn and Bacon.

Cohen, L.E., & Felson, M. (1979). Social Change and Crime Rate Trends: A Routine Activity Approach. *American Sociological Review,* 44(4), 588-608.

Egelman, S., Cranor, L.F., & Hong, J. (2008). *You've Been Warned: An Empirical Study of the Effectiveness of Web Browser Phishing Warnings*. New York: Assoc Computing Machinery.

Egelman, S., Molnar, D., Christin, N., Acquisti, A., Herley, C., & Krishnamurthi, S. (2010). Please Continue to Hold: An empirical study on user tolerance of security delays. In T. Moore & A. Friedman (Eds.), *The Ninth Workshop on the Economics of Information Security (WEIS) 2010*. Harvard University, USA.

Egelman, S., & Schechter, S. (2013). The Importance of Being Earnest [in Security Warnings]. In A.-R. Sadeghi (Ed.), *Financial Cryptography and Data Security 2013*. Okinawa, Japan: International Financial Cryptography Association.

Ert, E., & Erev, I. (2008). The rejection of attractive gambles, loss aversion, and the lemon avoidance heuristic. *Journal of Economic Psychology,* 29(5), 715-723.

Felson, M., & Clarke, R.V. (1998). Opportunity Makes the Thief: Practical theory for crime prevention. In B. Webb (Ed.), *Policing and Reducing Crime Unit: Police Research Series* (pp. 44). London, UK: Research, Development and Statistics Directorate.

Fischer, P., Lea, S., & Evans, K. (2009). The Psychology of Scams: Provoking and Commiting Errors of Judgement. Research for the Office of Fair Trading. In (pp. 260). Exeter, UK: University of Exeter.

Fischer, P., Lea, S.E.G., & Evans, K.M. (2013). Why do Individuals Respond to Fraudulent Scam Communication and Lose Money? The Psychological Determinants of Scam Compliance. *Journal of Applied Social Psychology [in press],* 43(10), 2060-2072.

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.

Gustafson, P.E. (1998). Gender differences in risk perception: Theoretical and methodological perspectives. *Risk Analysis,* 18(6), 805-811.

Halpern, S.D., Ubel, P.A., & Asch, D.A. (2007). Harnessing the Power of Default Options to Improve Health Care. *New England Journal of Medicine,* 357(13), 1340-1344.

Harwell, M. (2003). Summarizing Monte Carlo Results in Methodological Research: The Single-Factor, Fixed-Effects ANCOVA Case. *Journal of Educational and Behavioral Statistics,* 28(1), 45-70.

Herley, C. (2009). So Long, And No Thanks for the Externalities: The Rational Rejection of Security Advice by Users. In A. Somayaji & R. Ford (Eds.), *NSPW '09 Proceedings of the 2009 workshop on New security paradigms* Oxford, UK: ACM.

Herley, C. (2010). The plight of the targeted attacker in a world of scale. In T. Moore & A. Friedman (Eds.), *The Ninth Workshop on the Economics of Information Security (WEIS) 2010*. Harvard University, USA.

Jagatic, T.N., Johnson, N.A., Jakobsson, M., & Menczer, F. (2007). Social phishing. *Communications of the Acm,* 50(10), 94-100.

Johnson, E.J., Bellman, S., & Lohse, G.L. (2002). Defaults, Framing and Privacy: Why Opting In-Opting Out. *Marketing Letters,* 13(1), 5-15.

Jost, J.T., Banaji, M.R., & Nosek, B.A. (2004). A decade of system justification theory: Accumulated evidence of conscious and unconscious bolstering of the status quo. *Political Psychology,* 25(6), 881-919.

Kahan, D.M. (1997). Social Influence, Social Meaning, and Deterrence. *Virginia Law Review,* 83(2), 349-395.

Kahneman, D., Knetsch, J.L., & Thaler, R.H. (1991). Anomalies: The Endowment Effect, Loss Aversion, and Status Quo Bias. *Journal of Economic Perspectives,* 5(1), 193-206.

Kahneman, D., & Tversky, A. (1979). Prospect Theory: An Analysis of Decision under Risk. *Econometrica,* 47(2), 263-291.

Kim, D.J. (2008). Self-perception-based versus transference-based trust determinants in computer-mediated transactions: A cross-cultural comparison study. *Journal of Management Information Systems,* 24(4), 13-45.

Kirk, R.E. (2013). *Experimental design: Procedures for the behavioral sciences* (4th ed.). Thousand Oaks, CA: Sage.

Koslowsky, M., Schwarzwald, J., & Ashuri, S. (2001). On the Relationship between Subordinates' Compliance to Power Sources and Organisational Attitudes. *Applied Psychology: An International Review,* 50(3), 455-476.

Krol, K., Moroz, M., & Sasse, M.A. (2012). Don't work. Can't work? Why it's time to rethink security warnings. In *Risk and Security of Internet and Systems (CRiSIS), 2012 7th International Conference on* (pp. 1-8).

Lee, J.D., & See, K.A. (2004). Trust in automation: Designing for appropriate reliance. *Human Factors,* 46(1), 50-80.

Lix, L.M., Keselman, J.C., & Keselman, H.J. (1996). Consequences of Assumption Violations Revisited: A Quantitative Review of Alternatives to the One-Way Analysis of Variance F Test. *Review of Educational Research,* 66(4), 579-619.

Mariani, M.G., & Zappalà, S. (2006). Risk perception in online shopping. In S. Zappalà & C. Gray (Eds.), *Impact of e-commerce on consumers and small firms* (pp. 207- 222). Aldershot, England ; Burlington, VT: Ashgate.

Markus, H.R., & Kitayama, S. (1991). Culture and the self: Implications for cognition, emotion, and motivation. *Psychological Review,* 98(2), 224-253.

Modic, D. (2013). *Willing to be scammed: How self-control impacts Internet scam compliance.* Unpublished Research, University of Exeter, Exeter, UK.

Modic, D., & Lea, S.E.G. (2013). Scam Compliance and the Psychology of Persuasion [pre-print]. *Social Sciences Research Network,* Available at SSRN: http://ssrn.com/abstract=2364464.

Munro, A. (2009). *Bounded Rationality and Public Policy: A Perspective from Behavioural Economics* (Hardcover ed. Vol. 12). Tokyo: Springer Netherlands.

Murphy, K. (2004). The Role of Trust in Nurturing Compliance: A Study of Accused Tax Avoiders. *Law and Human Behavior,* 28(2), 187-209.

Osborne, J. (2010). Improving your data transformations: Applying the Box-Cox transformation *Practical Assesment, Research & Evaluation,* 15(12), 9.

Raven, B.H., Schwarzwald, J., & Koslowsky, M. (1998). Conceptualizing and Measuring a Power/Interaction Model of Interpersonal Influence1. *Journal of Applied Social Psychology,* 28(4), 307-332.

Rubinstein, A. (1997). *Modeling Bounded Rationality*. Boston: MIT Press.

Samuelson, W., & Zeckhauser, R. (1988). Status quo bias in decision making. *Journal of Risk and Uncertainty,* 1(1), 7-59.

Schmider, E., Ziegler, M., Danay, E., Beyer, L., & Bühner, M. (2010). Is It Really Robust? *Methodology: European Journal of Research Methods for the Behavioral and Social Sciences,* 6(4), 147-151.

Simon, H.A. (1956). Rational choice and the structure of the environment. *Psychological Review,* 63(2), 129-138.

Spool, J. (2011). Do users change their settings? . In J.M. Spool (Ed.), *User Interface Engineering* (Vol. 2013). www.uie.com: User Interface Engineering.

Stevenson, R.J. (2000). *The Boiler Room and Other Telephone Sales Scams*: University of Illinois Press.

Sunshine, J., Egelman, S., Almuhimedi, H., Atri, N., & Cranor, L.F. (2009). Crying Wolf: An Empirical Study of SSL Warning Effectiveness. In F. Monrose (Ed.), *The 18th USENIX Security Symposium*. Montreal, Canada: USENIX.

Tabachnick, B.G., & Fidell, L.S. (2005). *Using Multivariate Statistics* (5th ed.). Boston, MA: Allyn and Bacon.

Thaler, R.H., & Sunstein, C.R. (2008). Nudge : improving decisions about health, wealth, and happiness. In (pp. x, 293 p.). New Haven, Conn. ;London: Yale University Press.

Titus, R.M., & Dover, A.R. (2001). Personal Fraud: The Victims and the Scams. *Crime Prevention Studies,* 12, 133-151.

Triandis, H.C., Bontempo, R., Betancourt, H., Bond, M., Leung, K., Brenes, A., Georgas, J., Hui, C.H., Marin, G., Setiadi, B., Sinha, J.B.P., Verma, J., Spangenberg, J., Touzard, H., & Montmollin, G.d. (1986). The measurement of the etic aspects of individualism and collectivism across cultures. *Australian Journal of Psychology,* 38(3), 257-267.

Tyler, T.R., & Degoey, P. (1995). Collective restraint in social dilemmas: Procedural justice and social identification effects on support for authorities. *Journal of Personality and Social Psychology,* 69(3), 482-497.

Wu, J.J., & Tsang, A.S.L. (2008). Factors affecting members' trust belief and behaviour intention in virtual communities. *Behaviour & Information Technology,* 27(2), 115-125.

Zuckoff, M. (2005). Annals of Crime: The Perfect Mark. In *The New Yorker* (printed ed., Vol. 82, Iss. 13, pp. 36-42). New York, USA: Condé Nast, New York.