Nudging whom how: IT proficiency, impulse control and secure behaviour

Debora Jeske Lynne Coventry Pam Briggs
PaCT Lab, Psychology Dept.,
Northumbria University
Newcastle-upon-Tyne, UK
debora.jeske@northumbria.ac.uk
lynne.coventry@northumbria.ac.uk
p.briggs@northumbria.ac.uk

Aad van Moorsel
Computing Science
Newcastly University
Newcastle-upon-Tyne, UK
aad.vanmoorsel@ncl.ac.uk

ABSTRACT
This paper considers the utility of employing behavioural nudges to change security-related behaviours. We examine the possibility that the effectiveness of nudges may depend on individual user characteristics – which represents a starting point for more personalized behaviour change in security. We asked participants to select from a menu of public wireless networks, using colour and menu order to 'nudge' participants towards making more secure choices. The preliminary results from 67 participants suggest that while nudging can be an effective tool to help non-experts to select more secure networks, certain user differences may also play a role. Lower (novice level) IT proficiency and diminished impulse control led to poorer security decisions. At the same time, we were able to demonstrate that our nudge effectively changed the behaviour of participants with poor impulse control. We discuss these implications and pose several questions for future research.

Author Keywords
Behaviour change; Nudge; Personalization; Security.

ACM Classification Keywords
J.4 [Social And Behavioural Sciences]: Psychology.

INTRODUCTION
Personalization can be considered as a core component in behaviour change interventions. Recent interventions have adopted Thaler and Sunstein's (2008) popular approach to 'nudging' behaviour towards some desired outcome. Nudging tends to be directed towards a whole population and may use multiple nudges to achieve the same behaviour change rather than more fully understanding the relationship between the nature of the nudge and individual differences. The concept of nudging has proven so popular that the UK government has established a Behavioural Insights Team, colloquially known as the "Nudge unit" with the task of using insights from behavioural sciences to shape public policy in areas such as reducing energy consumption, providing honest tax returns and increasing the amount of money donated to charities. Nudging is increasingly used in the area of cyber security, where new choice architectures are being explored as a means of engineering better decision-making without the need to restrict choice or mandate behaviour change. However, in the security context, *personalized nudges* are still rare. Our study allows us to start to address the question of whether nudges have equal impact on different individuals.

"Personalizing Behavior Change Technologies" Workshop, CHI 2014, April 27, 2014, Toronto, Canada..

CYBER SECURITY: EXAMPLES OF NUDGES
To date, behavioural nudging has been investigated in terms of privacy in social media (Wang et al., 2013), on mobile devices (Balebako et al., 2011; Choe et al., 2013) and for general privacy (Acquisti, 2008). Ur et al. (2013) reported that a combination of visual and text feedback was the most effective intervention in the design of password strength meters. Choe et al (2013) also used visual framing to nudge individuals away from privacy-invasive apps. Our study aimed at studying the effectiveness of nudging users towards more secure wireless network selection. Wireless networks are becoming ubiquitous; however, as these are typically unsecured and unmonitored, they leave the users' systems vulnerable and open to security threats and attacks. But will nudges work effectively for all individuals, or do some depend upon the personal characteristics and attitudes of the end-user? In our study, we wanted to judge the extent to which nudges were effective but also explore the influence of user characteristics on the degree to which nudging is effective across different users.

DEVELOPING AND APPLYING NUDGES

We developed a set of nudges designed to steer a user towards secure wireless selection on android phones where the current default simply lists options alphabetically. Using the MINDSPACE framework (Dolan et al. (2012) to develop behavioural nudges, we focused on increasing salience by manipulating colour and menu order to address known selection bias (e.g., the propensity to pick the first menu option). We changed the order of networks to reflect their security status, placing the most secure options at the top. The colour nudge utilised a commonly used 'traffic light' colour scheme: labelling open (unsecure networks) red, secure networks orange, and trusted (as well as secure) networks green.

However, we also wanted to explore if a single nudge was effective, or if a combination was required. This gave us four nudges to evaluate: colour, order, colour and order, and the default option (no nudging). We also included a fifth option that included both nudges but no padlock to examine effect of perceived security or access (as our interest was to examine the influence of nudges on non-experts). We removed any potential effect of network familiarity and signal strength by creating random network names and presenting network options with the same number of bars. All screenshots included the same number of open (unsecure) network choices. The development of the nudge and the technical specifications are outlined in Turland et al. (under review).

Testing nudges

Our preliminary evaluation was conducted with 67 non-computing, university students who are familiar with using wireless networks on campus. This ensured that we had a representative sample of wireless network users with varying levels of IT proficiency. Forty participants completed a decision-making task and questionnaires in the laboratory, an additional 27 participants completed the task and measures using an online survey. All participants could earn research credits for their respective programs. We controlled accordingly for age, gender, and data collection method in our group comparisons.

Participants were given the following scenario: they have an hour to submit some urgent work and decide to go to a public café to connect to the Internet. In this context, they are presented with various network options. Participants were then asked to indicate their first choice from the available options on the five screen shots and to explain why they had picked specific networks in order to examine which features were effective. These explanations suggested that trusted implied secure for almost all participants. All images were randomly presented to reduce order effects.

In order to consider the effectiveness of our nudges in relation to user differences, following the decision-making task, all participants were asked to complete a survey. This survey collected demographics as well as information about IT proficiency, impulse control, technical and general privacy behaviours. Additionally, we asked all participants to tell us why they selected each option using an open response format. These comments were subsequently coded to better understand network access issues.

In the first step, we used Chi-square analysis to examine the overall effectiveness of our nudges. Specifically, we evaluated whether users' would pick more secure wireless networks depending on how the networks were presented on the screen. We found that nudging by order along was ineffective, but that colour could influence behaviour, leading to the selection of secure and trusted network options (p=.002). When colour and order were combined, 60% of participants selected secure options - a significant improvement on the default condition (p<0.001). An overview of the preliminary results is provided in Table 1.

	Participant choices	
Screenshots	**Open**	**secure/ trusted**
Networks not ordered by security, white labels (default Android)	49	18
Networks ordered, white labels	46	21
Networks not ordered, coloured	31	36
Networks ordered, coloured	27	40
Networks ordered, coloured, no padlock)	1	66

Table 1: Frequencies observed (N=67).

Further improvements were noticed when we compared the coloured as well as ordered results to the final and fifth screen shot featuring no padlocks. In the absence of a padlock, users also selected secure options almost 99% of the time, which suggests that part of the decision-making involved an assessment of the padlock. Open response options informed us that this effect may have been based on the fact that some users associated the padlock as a symbol for 'locked out' rather than 'security'. In the second step, we wanted to consider the influence of user differences.

RELEVANT USER CHARACTERISTICS

In order to assess how user characteristics might affect security choices, we scored each participant choice, with open (insecure) networks given 1 point and secure networks 2 points. This gave a range for each participant of 6 to 12 (with higher scores indicating more secure network selection). We then used these scores to assess a range of personal variables. The first background variable of interest here was IT proficiency as we assumed it should also relate to how secure or insecure participants' decisions are overall (in this case, in relation to wireless network selection).

IT proficiency

We observed the expected significant group difference based on IT proficiency after controlling for all covariates ($F(2,55)=4.573$, $p=.015$). Novices tended to make poorer decisions (M=6.87, SD=1.40, n=16) than participants who classified themselves as intermediate (M=7.95, SD=1.60, n=6) or at professional IT proficiency (M=8.33, SD=1.86, n=6). This indicates that self-judged IT proficiency was in line with different levels of more or less secure decisions made by our participants when selecting wireless networks.

The role of impulse control

We also wanted to examine if the extent to which our participants made more or less secure decisions overall (using the composite) was influenced by lack of impulse control. Impulse control has been examined in relation to internet addiction, poor employee behaviour and productivity (Yellowlees & Marks, 2007). In the context of security, poor impulse control creates an issue when employers rely on their employees to make careful decisions in order to keep their data and devices secure. This is particularly relevant when individuals need to access various wireless networks to access or transmit secure decisions. As a result, we also wanted to consider this variable as an important user characteristic when we try to nudge users into making better (secure decisions).

We used an item by Davis (2001) from the Diminished Impulse Control scale to assess impulse control. The item asked participants to rate on a five-point scale the extent to which they disagree-agree with the following: 'I use the internet more than I ought to'. Using regression, we observed a significant result (b= -.312, β = -.289, t= -2.175, p=.034, controlling for age, gender and data collection in the first step). The negative slope suggests that those with greater impulse issues are also more likely to make poorer security decisions overall.

In order to examine whether those with poorer impulse control were effectively nudged, we decided to categorise our users into two groups using a median split on the one-item measure (M=3.94). All participants who scored below this mean were considered to have good impulse control (n=14) in relation to their internet use. All participants who had a higher score on this item were considered to have poor impulse control (n=47). The groups at this stage were too small for statistical analyses (n<5). Six participants did not provide an answer to this question.

The results shown in Table 2 suggest some interesting possibilities. There is a trend of fewer and fewer participants choosing open (unsecure) wireless networks as we introduce different nudges. The change in responses suggests that nudging those with low impulse control appears to be more effective in changing their insecure behaviour while the effect of nudging those with good impulse control is relatively small, since most will also make better decisions without being nudged. Finally, removing the padlock has potential to influence everyone. This suggests that our intervention appears to change the behaviour in the right direction for those individuals who are also more likely to make less secure selection overall.

PRELIMINARY CONCLUSIONS

We can come to the following preliminary evaluation of our work: First, our results suggest that nudges can effectively and significantly change behaviour. Second, we also found evidence that user differences play a role in security decision-making. Third, our results further suggest that nudges can effectively change behaviour of those groups most likely to engage in insecure behaviours (e.g., those with poor impulse control). Lastly a combination is more effective than a single nudge.

	Wireless selection choices			
	Open		**Other (secure/ trusted)**	
Impulse control / **Screenshots**	Good	Poor	Good	Poor
Networks not ordered by security, white labels (default Android)	7 (50%)	39 (83%)	7 (50%)	8 (17%)
Networks ordered, white labels	8 (57%)	36 (77%)	6 (43%)	11 (23%)
Networks not ordered, coloured	4 (29%)	24 (51%)	10 (71%)	23 (49%)
Networks ordered, coloured	4 (29%)	21 (45%)	10 (71 %)	26 (55%)
Networks ordered, coloured, no padlock	0 (0 %)	1 (2%)	14 (100%)	46 (77%)

Table 2: Group statistics showing effect of nudging for participants with good and poor impulse control (N=61)

Of course, we readily acknowledge that our conclusions are preliminary and subject to a variety of limitations. We are still collecting data in order to increase cell group sizes as some of the comparisons were conducted with very small number of cases. We will also consider additional variables in future analyses.

POINTS FOR DISCUSSION

We believe that nudging has great utility for cyber security and that understanding the relationship between a specific nudge and user characteristics will help us be better able to predict who will benefit most from nudges. We would like to pose a number of questions regarding the issue of personalized nudging:

Which nudges are more likely to successfully change behaviour? And for whom? The MINDSPACE model by Dolan et al. (2012) provides a useful framework for brainstorming possible nudges as it outlines different ways in which behaviour is influenced - are there other frameworks out there that might be useful?

Does participatory design with potential recipients make a difference? Is the process of being involved in the discussions of the problem and the solutions a nudge in itself?

Does context matter? Health interventions and theories provide a useful starting point for interventions, however, we still know too little about which variables and frameworks can successfully be employed in a non-health setting such as security. The fact is that while most individuals agreeing to participate in health interventions are ready for change, we cannot assume the same for users of IT who behave insecurely. This creates an important gap to identify relevant variables (e.g., those that may translate from health to security) and possible transferable and generalizable findings across different disciplines.

What are the ethical considerations for nudging? Hint, nudge, push or shove - the question remains as to whether or not it is ethical to design systems to nudge people towards a particular behaviour, without those people consciously signing up to this behaviour change intervention?

REFERENCES

1. Acquisti, A. Nudging privacy. The behavioural economics of personal information. Security & Privacy Economics, Nov/Dec, (2009). 82-85.
2. Balebako, R., Leon, P.G., Almuhlmedi, H., Kelly, P.G., et al. Nuding users towards privacy on mobile phones. Procs of PINC2011: 2nd Int Workshop on Persuasion, Influence, Nudge & Coercion through mobile devices, May 8, Vancouver, Canada. (2011).
3. Behavioural Insights Team. Blog available at: http://blogs.cabinetoffice.gov.uk/behavioural-insights-team/category/uncategorized/. (2013)
4. Choe, E.K., Jung, J., Lee, B., & Fisher, K. Nudging people away from privacy-invasive mobile apps through visual framing. Procs of INTERACT 2013 Sep 2-6, Cape Town, South Africa. (2013)
5. Davis, R.A., Flett, G.L., & Besser, A. Validation of a new scale for measuring problematic internet use: Implications for pre-employment screening. CyberPsychology & Behavior, 5(4), (2002) 331-345.
6. Dolan, P. et al. Influencing Behaviour: The MINDSPACE way. Journal of Economic Psychology, 33, (2012) 264-277.
7. Thaler, R.H., & Sunstein, C.R. Nudge. Improving Decisions About Health, Wealth and Happiness. Penguin. (2008).
8. Ur, B., Kelley, P.G., Komanduri, S., et al. How does your password measure up? The effect of strength meters on password creation. In *Procs of the 21st USENIX conf on Security* (Security'12). USENIX Association, Berkeley, CA, USA, 5-5. (2012)
9. Wang, Y. Leon,P.D., Scott,K. Chen, X., Acquisti, A. & Cranor, L.F. Privacy nudges for social media: an exploratory Facebook study. In Procs of the 22nd int. conf. on World Wide Web, Switzerland, (2013) 763-770.
10. Turland, J., van Moorsel, A., Yevseyeva, I., Jeske, D., Coventry, L., & Briggs, P. Nudging towards secure wireless network selection. Manuscript under review. Mobile HCI (2014)
11. Yellowlees, P.M., & Marks, S. Problematic internet use or internet addiction? Computers in Human Behavior, 23, (2007) 1447-1453.

ACKNOWLEDGEMENTS

We would gratefully acknowledge the support and the contribution of our colleagues from Computing Science at Newcastle University who worked with us to identify issues and solutions and to develop an application of these nudges for Android phones. This research is supported by EPSRC Grant EP/K006568 Choice Architecture for Information Security, part of the GCHQ/EPSRC Research Institute in Science of Cyber Security.

AUTHOR BIOGRAPHIES

Lynne, Pam and Debora are all psychologists with a research history in behaviour change within different domains (security, health and learning respectively). They work together on this project looking at nudging as a means to improve security behaviours. They are all members of PaCT Lab – a group of researchers who are interested in psychological aspects of communication technology. Aad is a Head of Computing at Newcastle University whose team represent the other half of the project group. Their role is to consider security threats and the technical implementation of nudges.