BX 2017 Practitioner's Award Submission Form

Selected problem statement (please delete accordingly): ~~1~~/~~2~~/3

Project title

Should You Transfer That Cash?: Reducing Online Love Scams via Internet Banking Platforms

Authors

Daryl Tan: daryl.tan@u.yale-nus.edu.sg
Nicole Kuek: nicolekmy@gmail.com
Payal Lal: payallal93@gmail.com
Priscilla Tay: taypriscilla94@gmail.com
Rahul Naidu: rahulmarisar@gmail.com

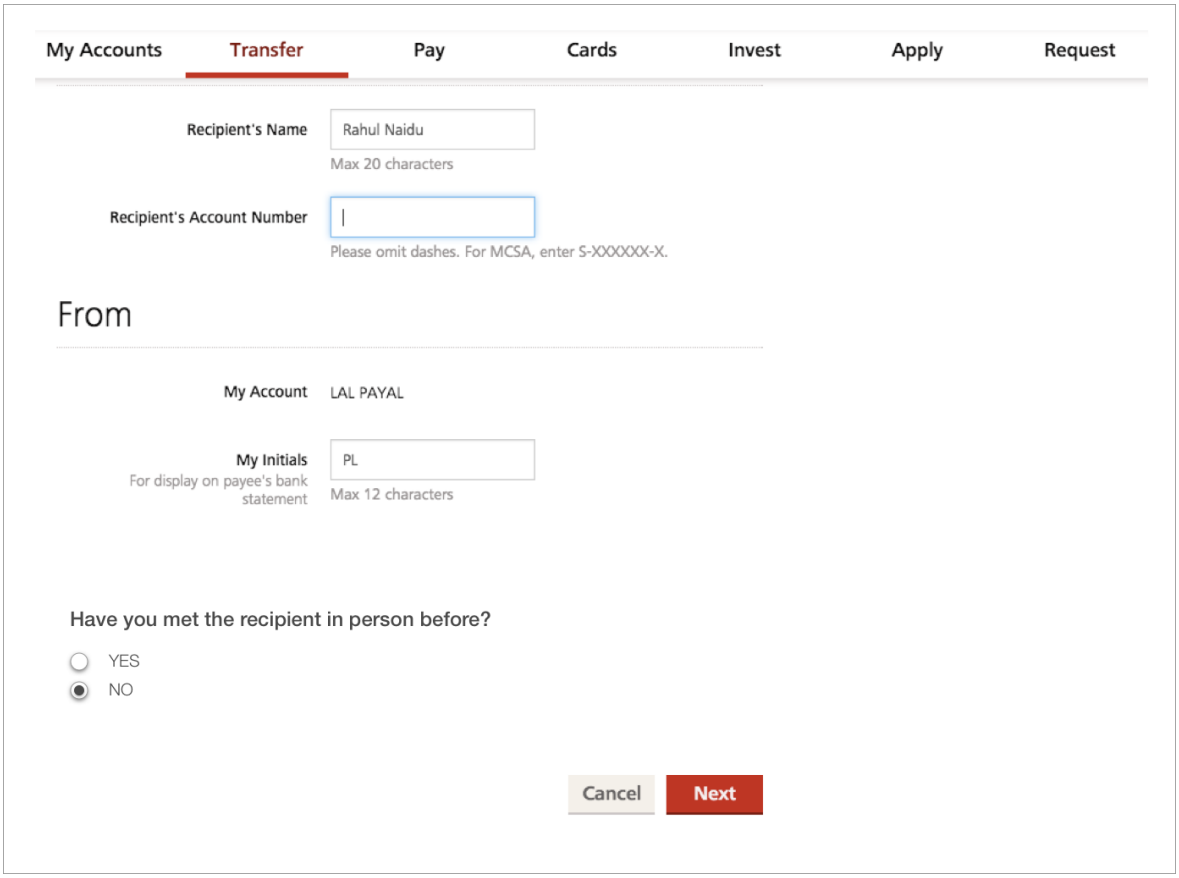
Answer to problem statement (300-500 words)

Guiding questions:

1. *What is the big idea behind the proposed solution? How does it address the problem?*
2. *What inspired this solution (e.g. practices from other countries; adapted from an existing concept)? How is this solution different from what has been tried before?*
3. *How do you measure and evaluate the outcomes of the intervention?*
4. *What resources are needed to deliver the solutions?*

In recent years, online love scammers have diversified methods of contacting potential victims ("Online love scammer changing tack", 2016) (e.g Tinder). Multinational conglomerates often have controlling interests in these platforms, making it difficult for local authorities to implement regulations. However, intervention at the level of national banks is still feasible. While we acknowledge victims of online love scams incur emotional, sexual and financial costs **(Whitty, 2015)**, our proposal specifically targets minimizing financial harm.

There is no shortage of existing scam warnings on the internet. However, their success is limited due to the lack of knowledge and unwillingness to consider oneself a potential target. POSB currently posts a single warning linked a long page on scams, and no direct links to report suspicious activity - which we find ineffective (see Figure 1).



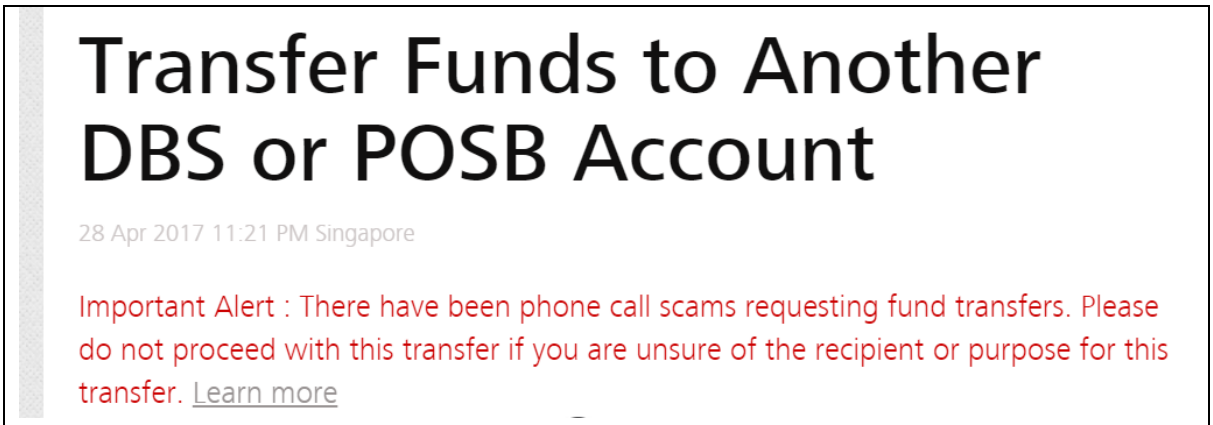


Figure 1. Current POSB scam warning.

Our intervention proposes to increase (1) **knowledge**, and (2) **salience** of potential scams, in order to encourage potential victims to recognize and report potential love scams. Studies suggest perpetrators of love scams avoid making real-life contact with victims (Whitty, 2015). Thus, (1) a checklist of typical scam behaviour (**knowledge-increasing**), (2) presented in a **salience-increasing** manner, *when bank transfers are made to unknown recipients*, can address the issue.

Upon initiating an online bank transfer to unknown recipients (see Figure 2), users are presented with a pop-up containing information about potential scams (see Figure 3).

Figure 2. If user states that they have not met the recipient in person before, the pop-up in Figure 3 appears.

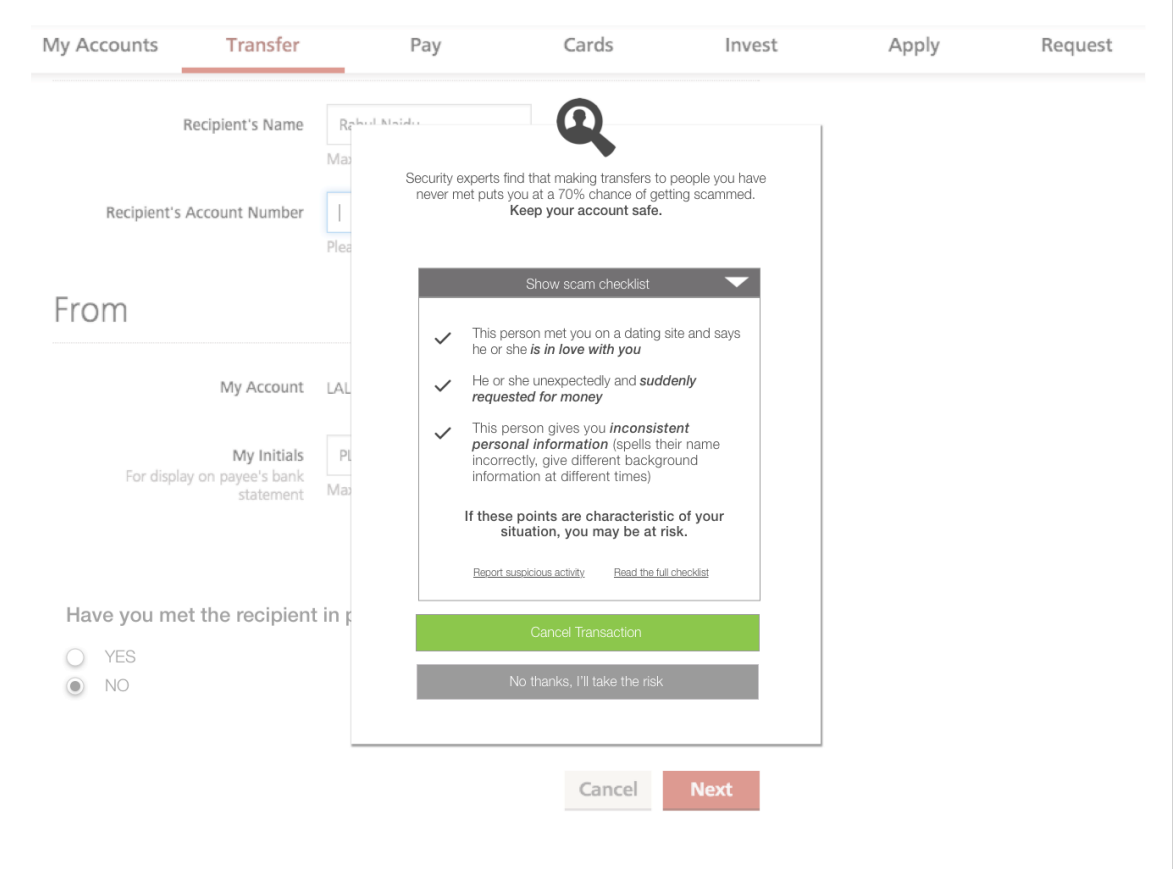


Figure 3. Pop-up presenting scam checklist and option to cancel the transaction.

For the pop-up design, principles from behavioural insights are utilized to increase awareness (via salience) of scams (see Figure 3):

(1) Increasing **credibility** of reports through citing "security experts" increases confidence in the information presented. **(Hovland, Janis, & Kelley, 1953)**

(2) Increasing **ease** of identifying and reporting scams through (A) short checklist and (B) button for reporting.

(3) Framing message as **potential loss** (i.e “70% chance of getting scammed”): per the **loss aversion principle,** users pay more attention to potential losses rather than benefits. **(Levin & Gaeth, 1988; Mellers, Chang, Birnbaum, & Ordóñez, 1992; also Schwarz, 1999)**

(4) Use of a **descriptive norm** that reminds users that they could also be victims of scams, increasing threat awareness. **(Goldstein & Cialdini, 2008)**

We propose testing this intervention via randomized controlled trials on a local internet banking platform (e.g. POSB) for a year. As the current interface does not have an option to report suspicious activity, we will add an additional Intervention Group for comparison for such an option (see Figure 4).

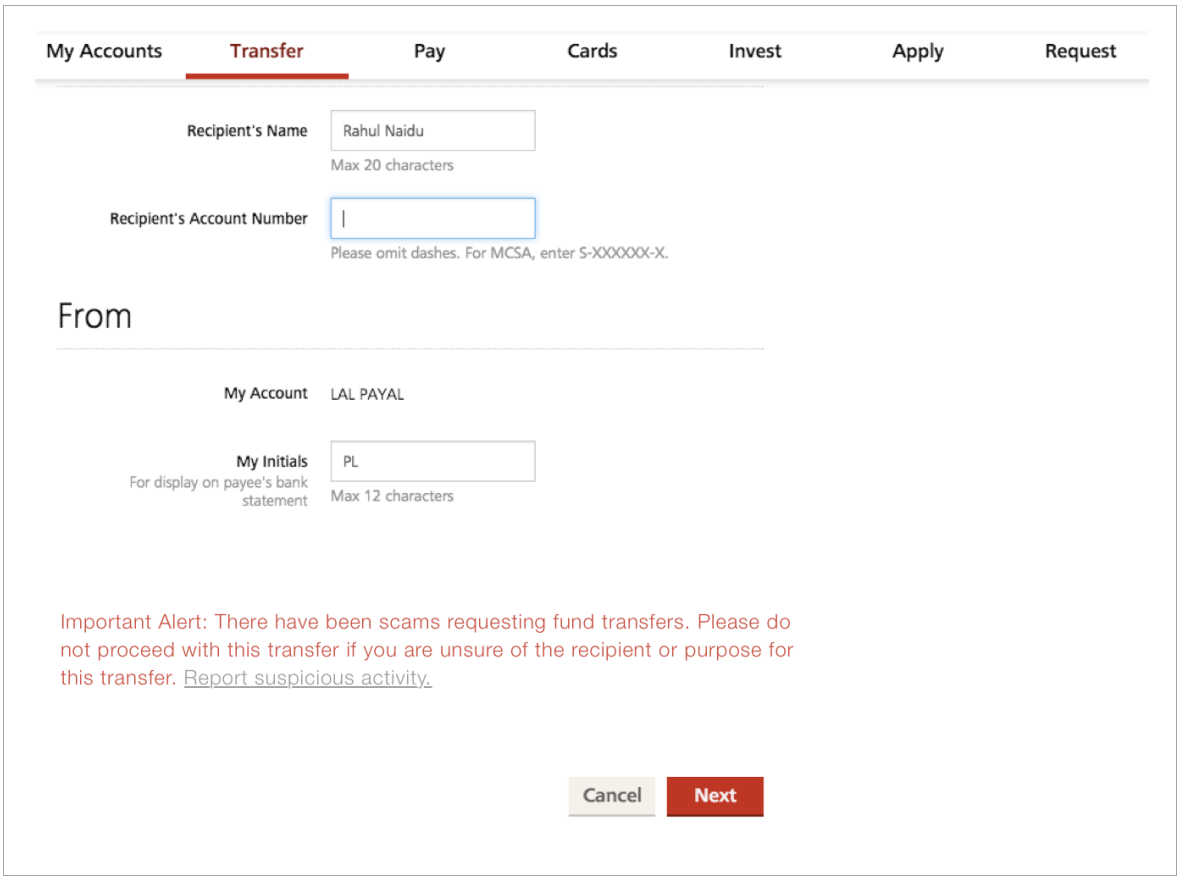
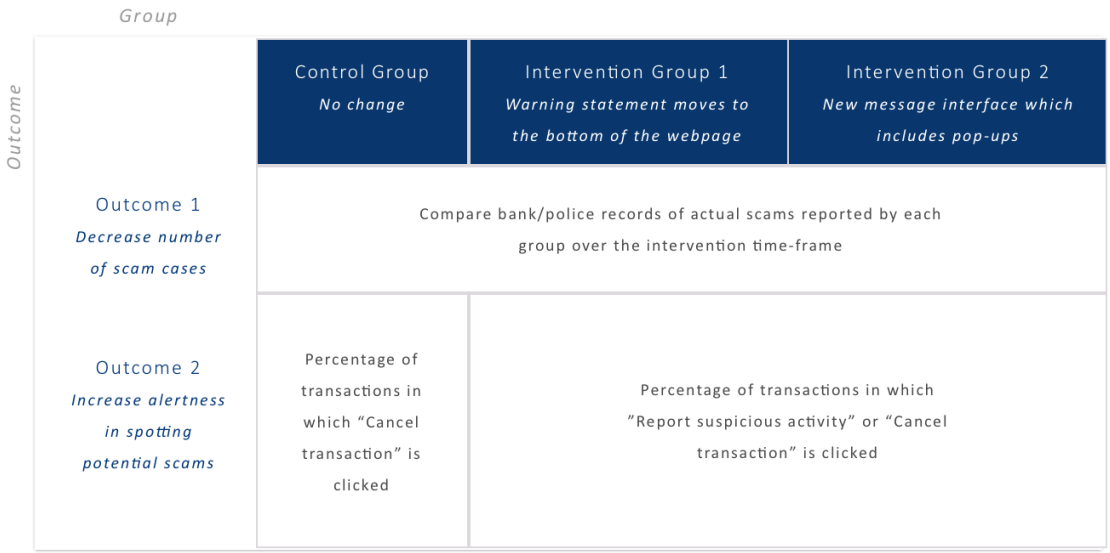


Figure 4. User interface for Intervention Group 1.

With local banks providing access to their site's programming, account holders could be randomly allocated to the three groups and presented with the respective interfaces. Average amount of time spent looking at the pop-ups in Intervention Group 2 could be used to check if users read the checklist. The intervention can be evaluated by measuring outcomes below:



References:

Ng, H. (2016, November 12). Online love scammer changing tack. *The Straits Times.*

Whitty, M. T. (2015). Anatomy of the online dating romance scam. *Security Journal*, *28*(4), 443-455

Hovland, C.I., Janis, I.L., & Kelley, H.H. (1953). *Communication and Persuasion*. New Haven, CT: Yale University Press.

Levin, I., & Gaeth, G. (1988). How consumers are affected by the framing of attribute information before and after consuming the product. *Journal of Consumer Research*, *15*, 374–378.

Goldstein, N., Cialdini, R., Griskevicius, V., & John Deighton served as editor and Mary Frances Luce served as associate editor for this article. (2008). A Room with a Viewpoint: Using Social Norms to Motivate Environmental Conservation in Hotels. *Journal of Consumer Research, 35*(3), 472-482.

*For submission, and/or any queries, please send them to: contact@bx2017.org