Journal of Economic Science Association manuscript No.
(will be inserted by the editor)

Real or bogus: Predicting susceptibility to phishing with economic experiments

Yan Chen · Iman Yeckehzaare · Ark Fangzhou Zhang

Received: date / Accepted: date

Abstract We present a lab-in-the-field experiment to demonstrate how individual behavior in the lab predicts their ability to identify phishing attempts. Using the business and finance staff members from a large public university in the U.S., we find that participants who are intolerant of risk, more curious, and less trusting commit significantly more false positive errors in an information security quiz. We also replicate prior results on demographics, including age, gender, and education level. Our results suggest that behavioral characteristics such as risk attitude, curiosity, and trust can be used to predict individual ability to identify phishing interfaces.

Keywords Risk aversion · Curiosity · Trust · Phishing

1 Introduction

The rapid evolution of information technology in recent decades has vastly changed our daily lives, from how we communicate with others to how we shop. However, the benefits of these technologies have come at the expense of our privacy and security. According to a recent survey by Wombat Security Technologies, the financial loss incurred due to successful phishing amounts to $4 million for an average 10,000-employee company.[1]

Yan Chen
School of Information, University of Michigan, 105 State Street, Ann Arbor 48109
E-mail: yanchen@umich.edu

Iman Yeckehzaare
School of Information, University of Michigan, 105 State Street, Ann Arbor 48109
E-mail: oneweb@umich.edu

Ark Fangzhou Zhang
School of Information, University of Michigan, 105 State Street, Ann Arbor 48109
E-mail: arkzhang@umich.edu

[1] `https://www.wombatsecurity.com/about/news/report-phishing-costs-average-organization-37-million-year`. Retrieved on September 17, 2016.

Various resources have been dedicated to reduce phishing susceptibility and most of these efforts focus on enhancing user awareness through warning systems. However, preventing a phishing attack depends not only on the technological sophistication of a system, but also on the personal characteristics that make some users more vulnerable to phishing attempts. Any phishing intervention requires an understanding of the personal characteristics that relate to the ability to recognize phishing attempts (Boyce et al., 2011). Indeed, when J.P. Morgan Chase & Co. sent a fake phishing email to its 250,000 employees, it found that 20% clicked on the bogus link.[2]

This paper presents a study that predicts participants' ability to distinguish phishing attempts from legitimate interfaces using behavioral attributes elicited in a series of economic experiments. Our participants are Business and Finance (B&F) staff members at a large public university in the U.S., whose work is commonly involved with sensitive data. The staff members are encouraged to participate in a phishing awareness education module developed by the Office of Information and Infrastructure Assurance (IIA) at the university. We add two research components to the education module. Before the education module, each participant takes a security quiz which includes seven questions, each of which asks the subjects to determine the legitimacy of an interface (website or email). Their answers are then used to determine their ability to identify phishing attempts. After completing the training module, they are invited to participate in a series of economic games designed to measure their risk attitude, trust and curiosity.

To our knowledge, this is the first study to provide predictions on individual susceptibility to phishing with their measured behavioral traits in a controlled laboratory experiment. Compared with prior studies on phishing – most of which use hypothetical scenarios, survey questions, or fake attacks to determine participants' behavioral attributes (Sheng et al., 2010; Costa and McCrae, 2008), our experiments can generate more precise and stable measurements of individual preferences that are representative of the population from which our participants are recruited (Cleave et al., 2013) and provide reliable out-of-sample predictions of individual behavior in the field (Tanaka et al., 2016; Karlan, 2005).

2 Experimental Design

Our study consists of two parts: an information security quiz with seven phishing-related questions and an incentivized economic experiment. To measure participants' risk attitude as well as their trust and curiosity, we include three economic games in our experiment: a lottery choice game (Holt and Laury, 2002), a gamble game (Eckel and Grossman, 2008), and a trust game (Berg et al., 1995). Each participant who chooses to participate in the experiment plays all the three games and is paid at the end of the experiment based

[2] https://www.wsj.com/articles/banks-battle-staffers-vulnerability-to-hacks-1450625921. Retrieved on September 17, 2016.

on her decisions as well as those of her match. The order of the games is randomized such that each participant is randomly assigned one of six possible orders.

2.1 The Information Security Quiz

We present participants with seven questions, each with an interface (website or email), which is either legitimate or bogus. We ask our participants to judge the legitimacy of the interface in each of the seven questions. The questions in the quiz are selected from two sources: (1) recent successful phishing attacks (such as university library access renewal, notification of a shared document, or an alert message from a bank account), and (2) questions with high error rates from a fall 2015 information security quiz administered to 5,892 students at the University of Michigan. The seven quiz questions are provided in the Appendix. This quiz is used to measure participants' ability to recognize phishing attempts, and is not incentivized per IIA request.

After completing the security quiz, the participants go through an interactive phishing awareness education module, which provides them with instructions on how to identify phishing attempts. This education module is designed by the IIA, and is not part of our study design. At the end of the education module, participants are invited to continue and complete an incentivized economic experiment with three games.

2.2 Economic games: Risk, curiosity and trust

Prior to our study, we conjecture that participants' risk preference, curiosity and trust might be good predictors of their susceptibility to phishing. We therefore adapt the lottery choice (Holt and Laury, 2002), the gamble (Eckel and Grossman, 2008) and the investment game (Berg et al., 1995) to measure these behavioral attributes, but in random order for each subject.

To elicit our participants' risk preferences, we use the Holt and Laury (2002) lottery choice game. To check the reliability and consistency of our measure for risk attitude, we also use the gamble developed by Eckel and Grossman (2008), which is a coarser but more intuitive measure of risk preferences.

At the end of the lottery choice game, the computer randomly selects one lottery to determine a participant's earnings. Participants are told their final earnings, but *not* which lottery is randomly chosen. Since the participants have already made their decisions and learned how much they have earned, the information on which lottery has been chosen has no instrumental value and the participants' willingness to pay (WTP) for it provides a measure for *curiosity* (Loewenstein, 1994; Golman and Loewenstein, 2015). This particular measure of curiosity is first developed in Chen and He (2015) as a reliable predictor for information acquisition behavior in the school choice context.

To elicit the participants' WTP for this non-instrumental information, we use the Becker-DeGroot-Marschak procedure (Becker et al., 1964; Benhabib et al., 2010) described as follows. The participants choose a number between 0 and 4 to indicate their WTP to learn the lottery that was selected. The computer then randomly picks a number uniformly between 0 and 4. If the number picked by the computer is less than the participant's WTP, the participant pays a price equal to the number and receives the lottery information. If the randomly-selected number is greater than the participant's WTP, she pays nothing and receives no information. In sum, the slight modification of the lottery choice game provides a measure of both risk preference and curiosity.

Lastly, we measure participant trust and trustworthiness using the investment game by Berg et al. (1995), but with the strategy method. In our version of the investment game, both the investor and the responder are given $5. An investor can transfer any amount from her initial endowment to the responder. The amount is then tripled by the experimenter before it is transferred to the responder. The responder can then transfer any amount back to the investor. With the strategy method, each participant submits her decisions first as an investor and then as a responder who decides how much to return contingent upon each possible investment.

To determine payoffs, we randomly match a participant to one of 41 subjects from a pilot session of the study and randomly assign the roles of the investor and the responder. Earnings are then calculated according to each participant's decision for the role to which she has been assigned. We use the strategy method to accommodate the asynchronous nature of participation in our online experiments.

2.3 Experimental procedure and participant characteristics

To conduct our study, we partner with the Office of Information Security Assurance (IIA) at the University of Michigan in their development of a phishing education module for the B&F staff. Before launching the study, the Chief Financial Officer of the university sends an email announcement to the B&F supervisors and staff, respectively, encouraging them to participate in the education module and research study. On April 14, 2016, we launched the study with an email to all B&F staff members that includes a link to the study website. The staff members can access the site with their university account, using the university authentication system. The study lasts for one month, during which a staff member can log onto our website at any time to participate. All B&F staff members are assured that their participation and responses will be anonymized and made available only to the researchers.

Out of the 3,190 B&F staff members, 1,201 participate in both the security quiz designed by the researchers and the security education module designed by the IIA staff. Of these, 811 staff members also participate in our economic experiment. Participants take on average 10 minutes and 2 seconds ($s.d.$ =

Table 1 Demographic Characteristics of Participants.

	Non participants	Quiz-NoGame	Quiz & Games
Age	46.68	50.25***	46.24
	(11.40)	(10.31)	(11.02)
Female (%)	36.24	53.74***	55.24***
White (%)	75.98	83.94	84.03***
High School or Lower(%)	32.64	13.85***	10.99***
Bachelor (%)	57.22	64.54***	64.53***
Post Graduate (%)	10.14	21.64***	24.48***
Salary (thousands)	61.01	76.27***	73.74***
	(30.84)	(37.38)	(38.72)
# obs	2298	361	764

Notes: ***denotes significance at the 1% level using the Wilcoxon rank-sum tests (for Age and Salary) and the binomial tests (for Female, White, High School or Lower, Bachelor, and Post Graduate) comparing the demographic characteristics between quiz participants and non-participants.

6.15 minutes) to finish all the components, with average earnings of $17.04 ($s.d. = \$6.04$) from the economic games.

In addition to the behavioral data, we obtain the participants' demographic data from the university's Human Resources Department. Among the 1,201 staff members who take the quiz, we are able to link 1,125 participants' behavioral data with their demographic information, including age, gender, ethnicity, education background, and annual salary.[3] Table 1 presents the summary statistics of demographic characteristics for the non-participants of the study (column "Non participants"), those who take the quiz but not the games (column "Quiz-NoGame") and those who take both the quiz and the economic games (column "Quiz & Games"). Comparing to the nonparticipants, We find that those who participate in the quiz represent a slightly older sample with a more balanced gender composition, larger proportion of whites, higher education levels, and higher annual salary. Among the B&F staffs who take the quiz, the demographic characteristics are balanced between those who participate in the games and those who do not.

Our main dependent variable is the participant quiz score, which is the number of correctly answered questions. The average score of the 1,201 B&F staff members is 4.97 out of 7.00, with a standard deviation of 1.25. We first investigate whether there is any sample selection bias by comparing the quiz scores of those who participate in the economic experiment and those who do not (Figure 1). We find no significant difference in the score distributions for the two groups ($p = 0.53$, two-sided Kolmogorov-Smirnov test).

We next examine the number of false positives (misidentifying a legitimate site) and false negatives (misidentifying a bogus site) in our quiz responses. Among the seven questions contained in the quiz, two reflect legitimate inter-

[3] Because the demographic dataset is obtained two months after the end of the study, it does not contain information for the 76 members due to staff turnover during those two months.

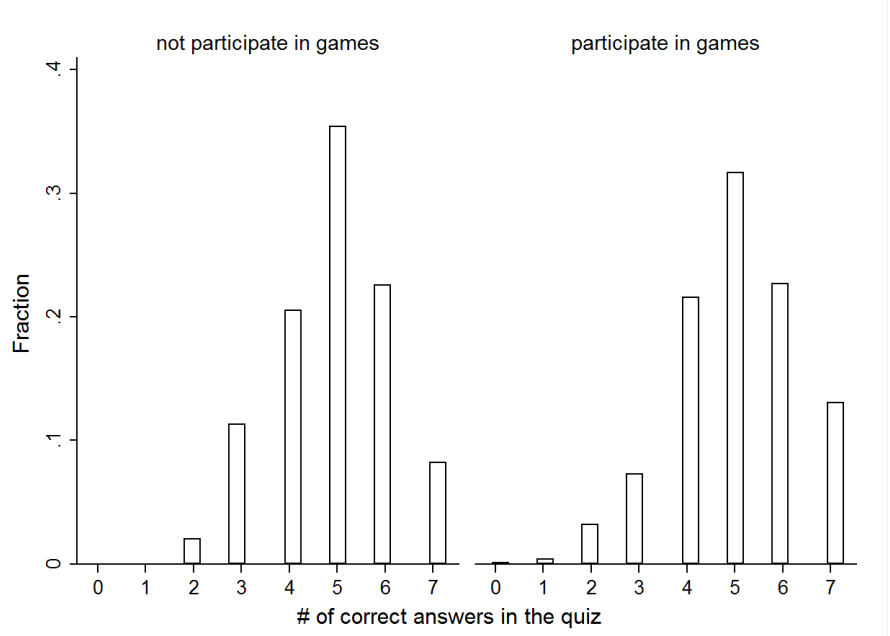


Fig. 1 Quiz score distributions among non-participants (left panel) and participants of economic games (right panel).

faces while five are bogus interfaces. Over 40% of our participants correctly identify all five phishing interfaces. Again, we find no significant difference in the number of false negatives between those who participate in the economic games and those who do not ($p = 0.99$, two-sided Kolmogorov-Smirnov test). In comparison, we find that nearly half our participants erroneously regard one legitimate interface as a phishing attempt and more than 30% misidentify both. Interestingly, those who do not participate in our economic games are marginally less likely to make false positive errors than those who do participate ($p = 0.08$, two-sided Kolmogorov-Smirnov test).

3 Results

In this section, we present how one's risk attitude, curiosity and trust predict one's ability to correctly identify phishing attempts.

We first look at risk attitude. The lottery game measures risk preference by varying the probabilities associated with a series of lotteries while holding the stakes of each lottery constant. We measure risk preference as the point when a participant switches from option A to option B. Following Holt and Laury (2002), we call those subjects who switch only once *consistent* subjects. Our results show that 66.5% of our participants are consistent. Among our inconsistent participants, we find that 28.8% switch multiple times and 10.2%

Table 2 Risk preference calibration and classification using consistent subjects ($n = 539$).

Switching Point in Lottery	CRRA Interval	Risk Preference Classification	Proportion from Lottery	Proportion from Gamble
1	$r < -1.6$	highly risk loving	7.9	n/a
2	$-1.6 \leq r < -1.1$	very risk loving	0.9	n/a
3	$-1.1 \leq r < -0.5$	risk loving	0.9	n/a
4	$-0.5 \leq r < 0.1$	risk neutral	11.0	27.5
5	$0.1 \leq r < 0.3$	slightly risk averse	20.0	0
6	$0.3 \leq r < 0.6$	risk averse	21.3	18.0
7	$0.6 \leq r < 0.9$	very risk averse	17.1	3.2
8	$0.9 \leq r < 1.3$	highly risk averse	7.6	11.5
9	$1.3 \leq r < 1.8$	extremely risk averse	1.3	0
10	$1.8 \leq r < 2.7$	intolerant of risk	11.5	39.7

Notes: n/a indicates that risk preference under this category cannot be captured by the gamble game by construction.

choose option A in the last row. This inconsistency may result from a lack of understanding, or from indifference in the case of multiple switching points.[4]

Table 2 displays the lottery switching point, the interval estimate for the implied constant relative risk aversion (CRRA) coefficient, the risk preference classification according to Holt and Laury (2002), and the corresponding proportion according to the choices from the gamble game. We find that nearly 10% of our subjects are risk loving, 11% are risk neutral, and 80% exhibit varying levels of risk aversion. Roughly 60% of the subjects switch to option B between the fifth and the seventh lottery, indicating a constant relative risk aversion coefficient in the range of $r \in [0.1, 0.9]$, which is in line with measurements from prior literature (Holt and Laury, 2002). Furthermore, we do not find statistically significant difference in switching point between genders (Cleave et al., 2013).

Our results from the gamble game are consistent with those from our lottery game. Specifically, we find that the Spearman's rank correlation coefficient between the switching point in the lottery and the choice number of the gamble is -0.28 ($p < 0.01$). Using a structural estimation, we find that the correlation between the CRRA coefficients inferred from the participants' choices in the two games is 0.38 ($p < 0.01$).

One interesting pattern observed in both games is that a substantial number of our subjects exhibit intolerance to risk by choosing the option that carries no uncertainty involved. In the lottery game, 11.5% of our subjects switch to option B in the last row, whereas no more than 1% of the subjects do so in Holt and Laury (2002). Likewise, 39.7% of our subjects choose the

[4] Inconsistency is commonly observed across various populations, typically correlated with the level of education. While it is typically low among college students (e.g., 5.8% among Danish undergraduates by Andersen et al., 2006; 13% among U.S. undergraduates by Holt and Laury, 2002), it is higher among working adults, especially those with lower levels of education (e.g., 36% among Shanghai workers with high school education by Chen et al., 2016, 41% among fishermen in South Africa by Brick et al., 2012, 55% among residents in Rwanda by Jacobson and Petrie, 2009).

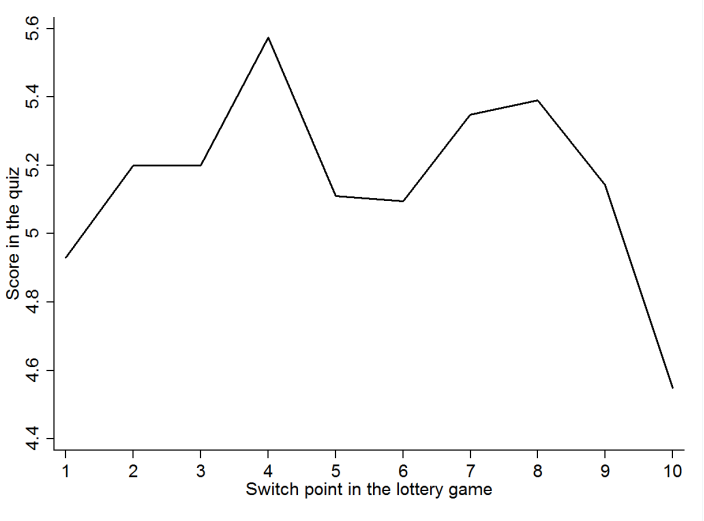


Fig. 2 Switching point in the lottery and average score in the quiz.

first option in the gamble game, compared to 10% in Eckel and Grossman (2008).

In Figure 2, we depict the average quiz score for the subgroup of consistent participants based on the switching point in the lottery game. This figure shows that those who are intolerant to risk are less likely to identify interfaces correctly. This establishes our first result.

Result 1 (Risk) *Individuals who are intolerant of risk achieve a significantly lower score on the information security quiz due to a greater number of false positive errors. Conditional on switching to option B in the first nine lotteries, the variation in risk attitude does not predict performance on the security quiz.*

Support: Table 3 report OLS and ordered logit regressions of quiz score over risk attitude - measured by the switching point and a dummy variable which equals one if a subject switches to option B in the 10^{th} lottery and zero otherwise. We find that switching to option B in the last lottery significantly decreases the score by nearly 0.60, with 0.38 of the decrease attributed to false negatives and 0.22 to false positives (Table 4) . The variation in the level of risk aversion, however, has an economically and statistically insignificant impact on the quiz score.

Result 1 shows that one's ability to correctly identify a phishing attempt may relate to risk attitude in whether one is willing to take any risk at all. Although option B provides a much higher expected payoff than option A in higher numbered lotteries, individuals who are intolerant of risk wait until the tenth and final lottery to switch, consistent with the finding that these individuals are more likely to make false positive errors.

Table 3 Regression of Security Quiz Score on Behavioral Attributes.

	OLS		Ordered Logit†	
	(1)	(2)	(3)	(4)
switching point	0.029	0.032	1.041	1.056
	(0.031)	(0.031)	(0.045)	(0.048)
I{switch at 10}	-0.766***	-0.599***	0.375***	0.454**
	(0.224)	(0.230)	(0.117)	(0.149)
curiosity	-0.094***	-0.071*	0.867***	0.089**
	(0.036)	(0.038)	(0.046)	(0.050)
trust	0.057*	0.038	1.086*	1.051
	(0.034)	(0.035)	(0.052)	(0.052)
age		-0.010**		0.982**
		(0.005)		(0.007)
female		-0.533***		0.415***
		(0.114)		(0.069)
R^2	0.039	0.089	0.014	0.033
# obs	539	506	539	506

† Odds ratios are reported.
Notes: *, **and ***denote significance at 10%, 5%, and 1% level. The regressions include only subjects whose choices are consistent in the lottery game. Results based on the full sample is available in the supplementary material.

Table 4 Regression of Number of False Positives and False Negatives in Security Quiz on Behavioral Attributes.

	False Positives				False Negatives			
	OLS		Ordered Logit†		OLS		Ordered Logit†	
switching point	-0.009	-0.011	0.976	0.968	-0.020	-0.022	0.958	0.954
	(0.018)	(0.017)	(0.044)	(0.046)	(0.025)	(0.026)	(0.043)	(0.044)
I{switch at 10}	0.475***	0.382***	3.424***	2.951***	0.292	0.217	1.680	1.446
	(0.128)	(0.128)	(1.142)	(1.045)	(0.183)	(0.190)	(0.553)	(0.503)
curiosity	0.047	0.029	1.130**	1.081	0.047	0.042	1.078	1.081
	(0.021)	(0.021)	(0.060)	(0.062)	(0.030)	(0.031)	(0.058)	(0.062)
trust	-0.049**	-0.041**	0.878**	0.890**	-0.009	0.003	0.097	0.995
	(0.019)	(0.019)	(0.044)	(0.047)	(0.028)	(0.029)	(0.047)	(0.051)
age		0.017***		1.047***		-0.007		0.989
		(0.003)		(0.008)		(0.004)		(0.007)
female		0.196***		1.729***		0.337***		2.061***
		(0.063)		(0.302)		(0.094)		(0.352)
R^2	0.060	0.135	0.029	0.073	0.010	0.037	0.004	0.018
# obs	539	506	539	506	539	506	539	506

† Odds ratios are reported.
Notes: *, **and ***denote significance at 10%, 5%, and 1% level. The regressions include only subjects whose choices are consistent in the lottery game. Results based on the full sample is available in the Appendix.

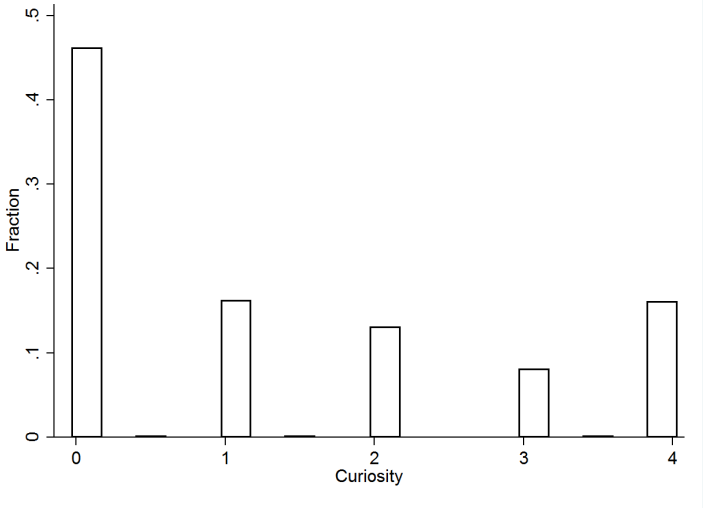


Fig. 3 Distribution of willingness-to-pay for non-instrumental information (curiosity).

We next investigate whether curiosity is correlated with the ability to identify phishing interfaces. Recall that we measure curiosity by a participant's willingness to pay for non-instrumental information, namely, which lottery is used to calculate her payoff. In Figure 3, we depict the distribution of subjects' willingness to pay in our experiment. Our results show that 55% of our subjects are willing to pay a positive amount to learn which lottery was chosen to determine their payoff. This finding is consistent with those from previous literature related to the endogenous information acquisition in the context of school choice (Chen and He, 2015), jury voting (Bhattacharya et al., 2015), and private value auctions (Gretschko and Rajko, 2015), which show that subjects have a tendency to overinvest in information acquisition.

Result 2 (Curiosity) *Individuals who exhibit a greater level of curiosity perform significantly worse in the information security quiz and are more likely to regard a legitimate interface as a phishing attempt.*

Support: In Table 3, we report the four regressions with curiosity as one of the independent variables. Results indicate that the number of correct answers on the quiz is negatively correlated to a participant's level of curiosity ($p < 0.01$, $p < 0.10$, $p < 0.01$, and $p < 0.05$, respectively). In Table 4, the parameter estimate for false positives is significantly greater than zero in column 3 ($p < 0.05$), suggesting that the more curious one is, the more likely she will regard a legitimate interface as bogus.

In addition to risk and curiosity, we measure how trusting our subjects are by the portion of a \$5 endowment they are willing to transfer to another participant who then has the option to transfer money back to the first participant. Our results show that the subjects transfer an average of \$2.85 (57%

of their initial endowment) with a median of $3. Fewer than 10% of our subjects choose not to transfer any money. Compared with previous experiments of trust game where subjects invest 51% of their endowment on average (see the meta-analysis by Johnson and Mislin, 2011), our results indicate that the B&F staff members in our sample appear to be more trusting than those in the previous studies. In Table 3, we report the parameter estimates from the OLS regression with the amount of money invested as an independent variable.

Result 3 (Trust) *More trusting participants answer marginally more questions correctly on the information security quiz. Furthermore, they are significantly less likely to regard a legitimate interface as a phishing attempt.*

Support: Columns 1 and 3 in Table 3 show that a participant's quiz score is positively correlated with the amount of money she chooses to transfer ($p < 0.10$). In Table 4, we find that they are significantly less likely to commit false positives ($p < 0.05$), indicating that those who transfer more money to a responder are less likely to misidentify legitimate interfaces as phishing attempts. Finally, we see that the regression using the number of false negatives generates a parameter estimate not significantly different from zero, suggesting that the level of trust does not relate to the tendency to commit false negatives.

Result 3 provides insights into how trust relates to individual performance in the information security quiz. It shows that more trusting participants are less likely to mark a legitimate interface as a phishing attempt.

Finally, Table 3 provides the analysis of the relationship between the performance on the quiz and demographics. The results in the last two rows show that the number of correct answers in the quiz is negatively correlated with participant age (-0.012, $p < 0.05$). This result supports previous findings that younger subjects are more likely to correctly identify phishing attempts (Sheng et al., 2010; Kumaraguru et al., 2009). In addition, older participants are more likely to regard legitimate emails as phishing (0.017, $p < 0.01$, Table 4). Regarding gender, the last row in Table 3 suggests that females score lower than males (-0.520, $p < 0.01$), with 36% attributed to false positives and 64% attributed to false negatives ($p < 0.01$ in all specifications, Table 4).

4 Conclusion

This paper explores how phishing susceptibility relates to measurable behavioral attributes, such as risk preference, curiosity, and trust. Using a lab-in-the-field experiment with staff members in the business and finance department of a large public university, we find that individuals who are intolerant of risk are more likely to regard legitimate interfaces as phishing. By contrast, we find that participants who are more trusting and less curious perform better on a security quiz. Our findings also reinforce those in previous research that older participants provide more incorrect answers as do females when compared to males. Finally, we provide a greater understanding of how behavioral traits relate to the ability to identify phishing attempts by decomposing the

incorrect responses into false negatives and false positives. Our findings thus enhance our understanding of users' ability to identify phishing attempts and suggest that the lottery choice game can be modified and incorporated into the design of phishing education programs. Individuals who switch to the B option in the last lottery (intolerant to risk) and individuals whose WTP for non-instrumental information is high (more curious) are likely to misidentify the legitimacy of emails or websites. Our paper suggests that individual choices in the modified lottery game can be used as a stable diagnostic tool to identify potential victims to the ever evolving phishing techniques.

Acknowledgements We thank Sol Bermann, Janet Eaton, Matthew Kay, Nancy Kotzian, Florian Schaub, Gregory Stathes, and Denise Stegall for helpful discussions and comments. Financial support from the IIA at the University of Michigan is gratefully acknowledged.

References

Andersen S., Harrison G. W., Lau M. I., Rutström E. E. (2006) Elicitation using multiple price list formats. Experimental Economics 9(4):383–405

Becker G. M., DeGroot M. H., Marschak J. (1964) Measuring utility by a single-response sequential method. Behavioral Science 9(3):226–232

Benhabib J., Bisin A., Schotter A. (2010) Present-bias, quasi-hyperbolic discounting, and fixed costs. Games and Economic Behavior 69(2):205–223

Berg J., Dickhaut J., McCabe K. (1995) Trust, reciprocity, and social history. Games and Economic Behavior 10(1):122–142

Bhattacharya S., Duffy J., Kim S.-T. (2015) Voting with endogenous information acquisition: Theory and evidence. Tech. rep.

Boyce M. W., Duma K. M., Hettinger L. J., Malone T. B., Wilson D. P., Lockett-Reynolds J. (2011) Human performance in cybersecurity a research agenda. In: Proceedings of the Human Factors and Ergonomics Society Annual Meeting, SAGE Publications, vol 55, pp 1115–1119

Brick K., Visser M., Burns J. (2012) Risk aversion: experimental evidence from south african fishing communities. American Journal of Agricultural Economics 94(1):133–152

Chen Y., He Y. (2015) Information acquisition and provision in school choice. Tech. rep., mimeo

Chen Y., Jiang M., Krupka E. (2016) Hunger and economic decision-making: A direct test, university of Michigan Working Paper

Cleave B. L., Nikiforakis N., Slonim R. (2013) Is there selection bias in laboratory experiments? the case of social and risk preferences. Experimental Economics 16(3):372–382

Costa P. T., McCrae R. R. (2008) The revised neo personality inventory (neo-pi-r). The SAGE handbook of personality theory and assessment 2:179–198

Eckel C. C., Grossman P. J. (2008) Men, women and risk aversion: Experimental evidence. Handbook of experimental economics results 1:1061–1073

Golman R., Loewenstein G. (2015) Curiosity, information gaps, and the utility of knowledge. Information Gaps, and the Utility of Knowledge (April 16, 2015)

Gretschko V., Rajko A. (2015) Excess information acquisition in auctions. Experimental Economics 18(3):335–355

Holt C. A., Laury S. K. (2002) Risk aversion and incentive effects. American Economic Review 92(5):1644–1655

Jacobson S., Petrie R. (2009) Learning from mistakes: What do inconsistent choices over risk tell us? Journal of Risk and Uncertainty 38(2):143–158

Johnson N. D., Mislin A. A. (2011) Trust games: A meta-analysis. Journal of Economic Psychology 32(5):865–889

Karlan D. S. (2005) Using experimental economics to measure social capital and predict financial decisions. American Economic Review 95(5):1688–1699

Kumaraguru P., Cranshaw J., Acquisti A., Cranor L., Hong J., Blair M. A., Pham T. (2009) School of phish: a real-world evaluation of anti-phishing training. In: Proceedings of the 5th Symposium on Usable Privacy and Security, ACM, p 3

Loewenstein G. (1994) The psychology of curiosity: A review and reinterpretation. Psychological Bulletin 116(1):75

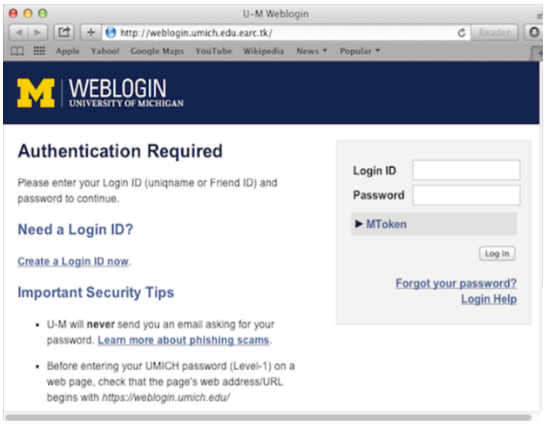
Sheng S., Holbrook M., Kumaraguru P., Cranor L. F., Downs J. (2010) Who falls for phish?: a demographic analysis of phishing susceptibility and effectiveness of interventions. In: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, ACM, pp 373–382

Tanaka T., Camerer C. F., Nguyen Q. (2016) Risk and time preferences: Linking experimental and household survey data from vietnam. In: Behavioral Economics of Preferences, Choices, and Happiness, Springer, pp 3–25

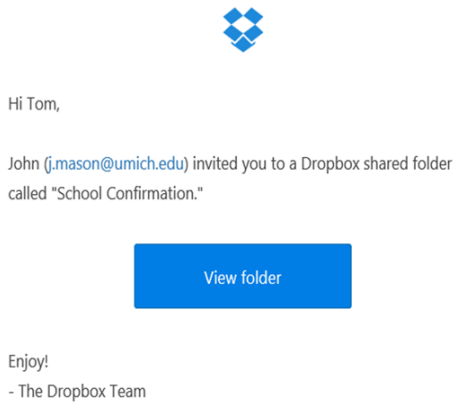
Appendix (for online publication only)

A.1 The Information Security Quiz

1. You receive an email urging you to click the link below to renew your X Library privileges:
   www.umich.edu/renew-library-privileges
   Is this a legitimate website?
2. Suppose you have a bank account with Wells Fargo and receive an email asking you to click the link below:
   https://www.wellsfargo.com/
   Is this a legitimate link?
3. You receive an email that claims your library access will expire soon. It links to the site depicted. Is it safe to enter your username and password?



4. You have an account with Amazon and receive an email asking you to click the link below:
   http://www.amazon.com.varzeas.us
   Is this a legitimate link?
5. You have an account with Citibank and receive an email asking you to click the link below:
   http://www.citibanking.net
   Is this a legitimate link?
6. Suppose Tom received an email from a friend that says a document has been shared with him on Dropbox. The email is shown below. Do you think Tom should click the "view folder" button?



7. You have an account with Amazon and receive an email asking you to click the link below:
http://www.amazon.co.uk
Is this a legitimate link?

A.2 Additional Analyses for Robustness Check

Table 5 OLS Regressions of Performance in Quiz for the Full Sample.

	Score		# False Pos.		# False Neg.	
switching point	-0.004	0.003	0.010	0.007	-0.006	-0.011
	(0.023)	(0.023)	(0.013)	(0.013)	(0.019)	(0.019)
I{switch at 10}	-0.474**	-0.377*	0.318***	0.255**	0.156	0.122
	(0.192)	(0.195)	(0.110)	(0.109)	(0.159)	(0.164)
curiosity	-0.073**	-0.042	0.039**	0.020	0.034	0.023
	(0.029)	(0.030)	(0.017)	(0.017)	(0.024)	(0.025)
trust	0.053*	0.019	-0.039**	-0.026	-0.013	0.007
	(0.028)	(0.028)	(0.016)	(0.016)	(0.023)	(0.024)
age		-0.012*		0.019***		-0.006*
		(0.004)		(0.002)		(0.004)
female		-0.543***		0.197***		0.346***
		(0.094)		(0.053)		(0.079)
R^2	0.019	0.074	0.028	0.126	0.000	0.026
# obs	811	764	811	764	811	764

Notes: *, **and ***denote significance at 10%, 5% and 1% level using t test. The regressions include all subjects. The switching point of the inconsistent subjects are defined as the mid-point between their first switching point and their last switching point.

Table 6 OLS Regressions of Performance in Security Quiz over Risk Attitude Elicited from the Gamble Game.

	Sub-sample of Consistent Participants				Full Sample			
	Score	Score	# False Pos.	# False Neg.	Score	Score	# False Pos.	# False Neg.
chosen gamble	-0.032	-0.037	0.003	0.033	-0.012	-0.021	0.001	0.021
	(0.027)	(0.027)	(0.015)	(0.022)	(0.021)	(0.021)	(0.012)	(0.018)
I{choose gamble 1}	-0.336*	-0.266	0.086	0.181	-0.121	-0.149	0.070	0.079
	(0.183)	(0.187)	(0.104)	(0.153)	(0.145)	(0.145)	(0.081)	(0.121)
age		-0.016***	0.022***	-0.006		-0.014***	0.020***	-0.005
		(0.005)	(0.003)	(0.004)		(0.004)	(0.002)	(0.004)
female		-0.562***	0.219***	0.343***		-0.564***	0.214***	0.350***
		(0.116)	(0.065)	(0.095)		(0.093)	(0.052)	(0.078)
R^2	0.003	0.060	0.120	0.025	0.000	0.069	0.115	0.028
# obs	539	506	506	506	811	764	764	764

Notes: *, **and ***denote significance at 10%, 5% and 1% level using t test. The left panel includes only the subjects whose choices in the lottery game are consistent. The right panel includes all the subjects.

A.3 Decisions in the Trust Game from the Pilot Study

Subject No.	Investment	Return 0	Return 1	Return 2	Return 3	Return 4	Return 5
1	5	0	0	0	1	1	2
2	5	0	2	4	7	9	10
3	3	0	1	2	4	5	7
4	0	0	0	0	0	0	0
5	2	0	0	0	1	0	5
6	4	0	2	3	6	8	8
7	5	5	3	2	3	7	10
8	3	0	2	3	4	6	8
9	1	0	0	0	0	0	0
10	2	2	2	1	3	3	5
11	0	0	2	4	6	8	10
12	5	0	1	3	5	7	10
13	2	0	1	2	3	5	5
14	2	2	3	5	7	8	10
15	1	0	0	0	0	0	0
16	2	0	2	4	6	7	10
17	1	0	0	0	3	5	7
18	3	0	2	4	5	7	8
19	5	3	1	1	2	4	6
20	2	0	1	2	3	4	5
21	1	5	7	0	1	3	5
22	1	0	1	3	4	6	8
23	1	1	2	4	6	8	10
24	1	0	1	1	1	1	1
25	3	1	1	1	2	2	2
26	2	1	1	3	4	5	9
27	2	0	1	2	4	6	10
28	0	0	1	4	6	8	10
29	0	1	3	4	3	4	5
30	2	0	1	4	5	7	10
31	0	0	1	2	3	4	5
32	0	0	0	0	0	0	0
33	1	1	2	3	2	2	2
34	4	2	2	2	4	5	4
35	2	2	3	4	4	5	7
36	4	3	5	7	9	10	11
37	5	5	8	11	7	8	10
38	5	0	0	0	0	0	6
39	1	0	2	0	0	0	0
40	1	0	1	2	3	4	5
41	3	1	2	4	6	9	11

A.4 The Games Interfaces

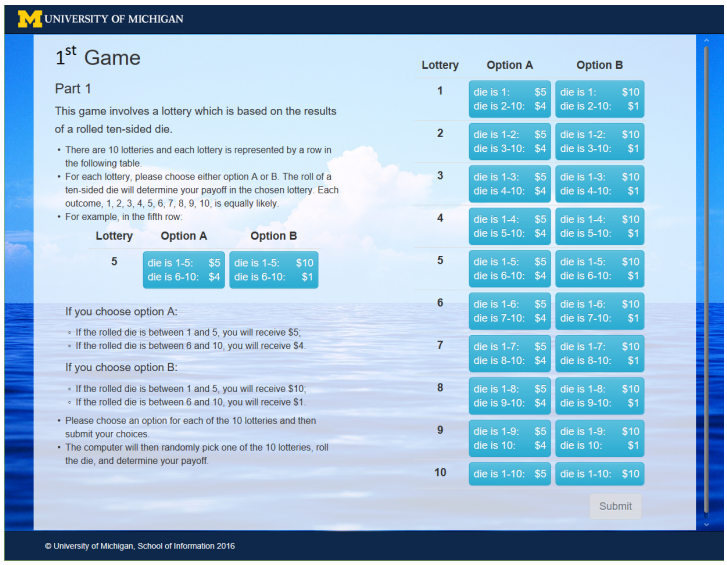


Fig. 4 The Holt-Laury Lottery Choice Game Interface.

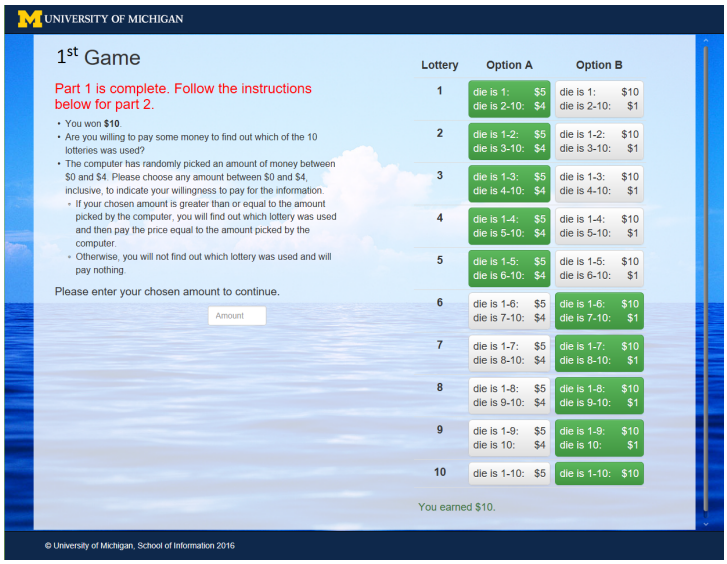


Fig. 5 The Curiosity Measurement Interface.

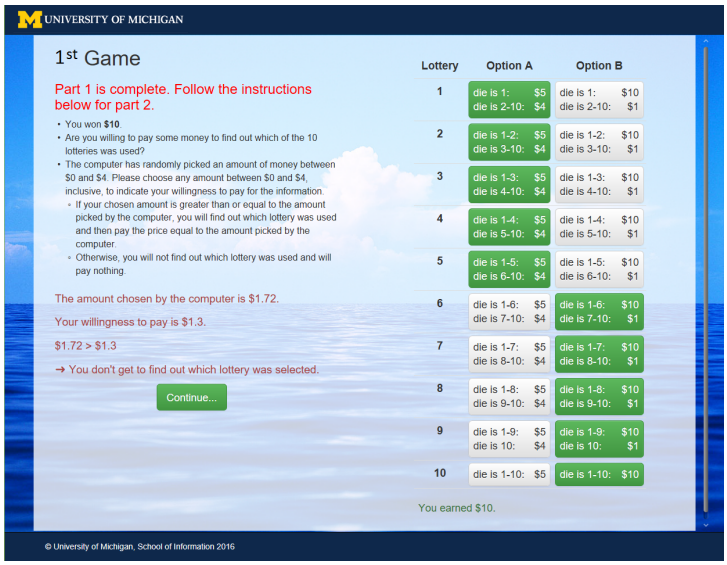


Fig. 6 The Curiosity Result Interface.

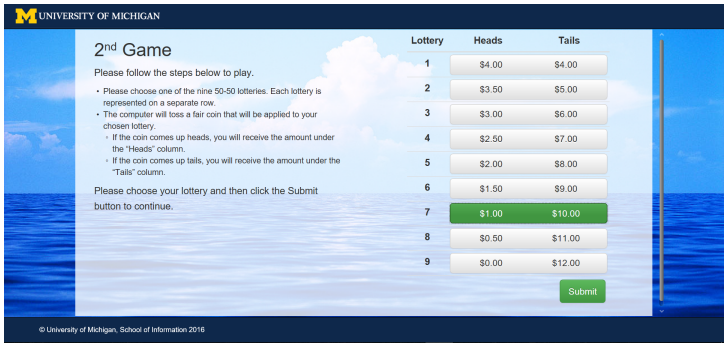


Fig. 7 The Eckel-Grossman Gamble Interface.

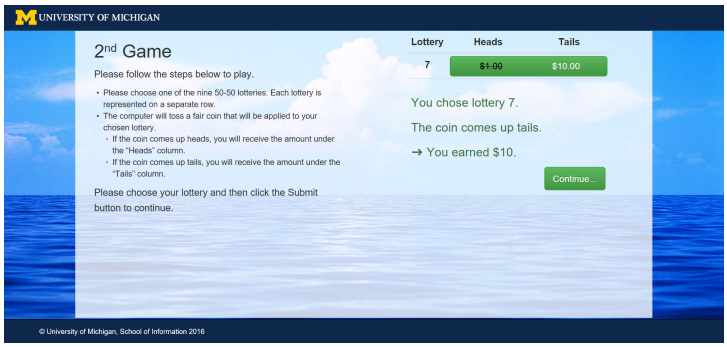


Fig. 8 The Eckel-Grossman Gamble Result Interface.

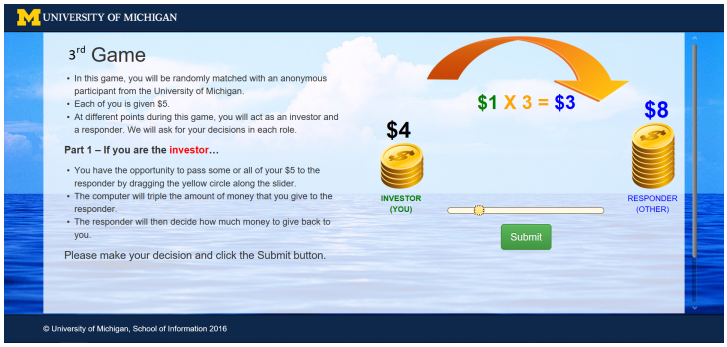


Fig. 9 The trust Investment interface.

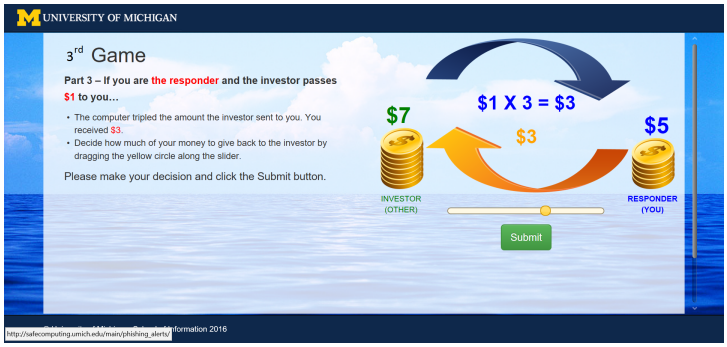


Fig. 10 The Trust Response Interface.

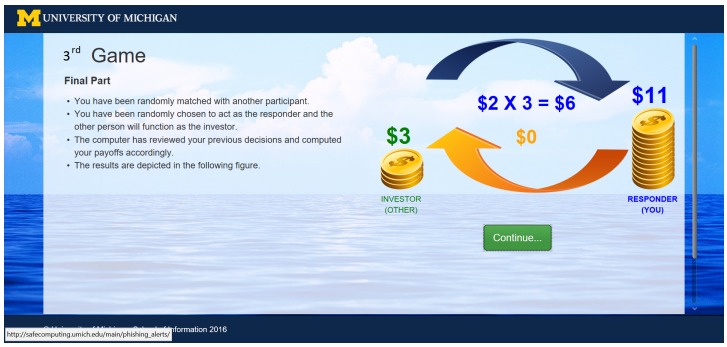


Fig. 11 The Trust Result Interface.

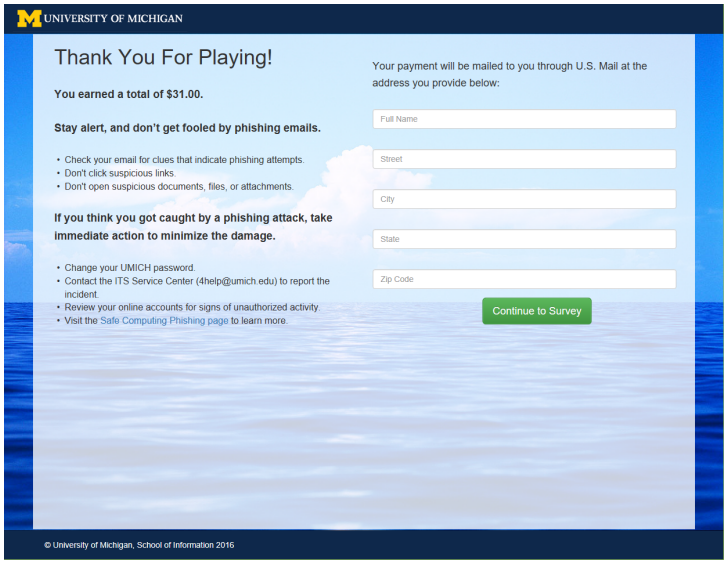


Fig. 12 The Thank-you Interface.

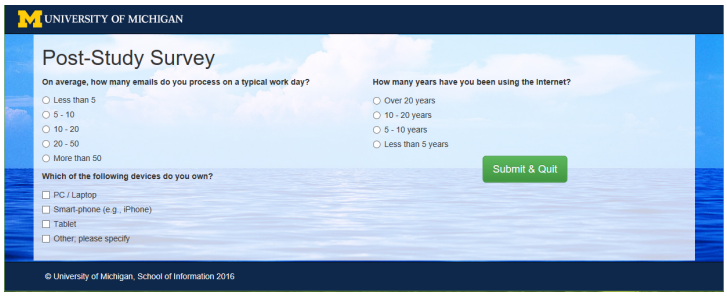


Fig. 13 The Survey Interface.