Completed Paper

**Nature vs. Nurture: The Genetic Basis of Behavioral Security**

Tingting (Rachel) Chung

Chatham University

Dennis Galletta

University of Pittsburgh

We would like to thank the Institute for Fraud Prevention (IFP), Carlow University’s Geibel Institute for Social Justice and Responsibility, and the Dean’s Office at Katz Graduate School of Business of the University of Pittsburgh for financial support for this research. We would also like to thank Jennifer Bourne, David Carroll, Manika Kumari, Michelle Lu, Chenjui Su, Amy Timo, Jocelyn Inlay, and Sook Yee Leung for their assistance with data collection and management. Earlier versions of this paper have been presented at the IFP Summer 2013 meeting, and the Pre-ICIS HCI Workshop 2013.

**Nature vs. Nurture: Genetic Basis of Behavioral Security**

**Abstract**

Behavioral genetics offers numerous opportunities to bridge gaps in biological research of organizational science and to shed light on the nature versus nurture debate. This study seeks to explain persistent vulnerability to behavioral security from a genetic perspective. A synthesis of current literatures on cognitive neuroscience, decision making, and behavioral security suggests that there may potentially be a genetic basis for user susceptibility to security risks. Using the classic twin design, this study reports estimated heritability of behavioral security to be up to 36% by comparing concordance between 144 pairs of monozygotic (MZ) twins and that between 98 pairs of same-sex dyzygotic (DZ) twins on a behavioral security test. The results suggest that behavioral security is explained largely by both shared and non-shared environmental influences. Zygosity of the twin pairs serves as the primary independent variable in these behavioral genetics analyses. Implications of the study results are discussed with respect to anti-fraud research as well as managerial practices.

# Introduction

Vulnerabilities to behavioral security are present in both personal realms and business settings. According to a 2012 PricewaterhouseCoopers report, 82% of large organizations suffer from staff-initiated security incidents (Potter and Waterfall 2012). Similarly, a 2013 research report by the Ponemon Institute (Ponemon\_Institute 2013) suggests that 64% of information security breaches in 2012 resulted from human errors in addition to systems problems. For example, employees at the grocery chain SuperValu received a phishing message indicating new (fraudulent) wire transfer account numbers for two vendors, Frito-Lay and American Greetings. The employees complied and sent $10 million to the bogus accounts[[1]](#footnote-1). Such security vulnerability issues are of particular concern when entire enterprises are being built on digital infrastructures.

Synthesizing both academic research and government reports (Consumer\_Fraud\_Research\_Group 2006; Grazioli and Jarvenpaa 2003; Office\_of\_Fair\_Trading 2009; Titus et al. 1995), we define behavioral security, as the extent to which the user is able to prevent malicious compromises to data privacy, confidentiality, or integrity. Our definition expands on the general notion of deceit traditionally explored in the literature. For example, it is common to find phishing messages that purport to confirm a delivery or offer a personal meeting that could lead to a romantic date. A person could even be a fraud victim by receiving an electronic message that says “hey, check this out” (Jagatic et al., 2007). As such, behavioral security can be compromised through both traditional (e.g., face-to-face interactions, postal mail) and electronic (e.g., electronic mail, social media, e-commerce websites) channels.

Researchers have concentrated on two major aspects of computer security. The first area of study involves controls and systems, which include tools for encryption, identity assurance, and threat discovery and elimination. However, as the SuperValu case illustrates, the human element can be the weakest link even in well-established organizations. The second area of security research, therefore, focuses on the human element, examining two groups of people involved in the threats: the perpetrators and the victims. Studies of perpetrators attempt to predict the likelihood of unleashing a threat, identify their identity, and dissuade people from carrying out attacks by threatening likely and severe punishment. Studies of victims, however, investigate what kinds of attacks are most persuasive (e.g., Dhamija et al. 2006), who might fall for these attacks (e.g., Jagatic et al., 2007; Galletta, et al., 2011), and how people might be better armed against them (e.g., (Kirlappos and Sasse 2012).

Rational methods to arm people against attacks would be to motivate people through education or training. However, the effectiveness of these methods has been rather disappointing so far. For example, Weirich (2006) found no significant differences between two groups in their responses to a survey questionnaire five months after fear appeals were administered, thus concluding that similar training methods may be ineffective for fraud prevention in an organizational setting. Herley (2009) demonstrated that the estimated costs of learning safe computing methods outweigh the actual benefits, making it difficult for people to justify investing the time in proper safety precautions. User education focusing on specific indicators of Internet safety (e.g., the VeriSign,the padlock symbol) is often unsuccessful because users often possess misconceptions about Internet safety that go above and beyond specific indicators. Many such misconceptions reflect deep-rooted decision making heuristics and biases, such as trust halo effect or anchoring effect, rather than a simple lack of knowledge (Kirlappos and Sasse 2012).

Though education and training have shown little promise to date, it is striking that some people are more vulnerable to security risks than others. Some pay attention to red flags that others miss, and still others continue to fall for the scam despite repeated training efforts. Because our knowledge and behavior differ so widely, and the consequences of risky behaviors can be serious, it is important to focus carefully on this issue. Why is it so difficult to share that knowledge and also motivate more people to avoid becoming victims? In many fields, especially psychology and medicine, when individual differences puzzle researchers, it is natural to determine the extent to which nature (i.e., genetics) is more important than nurture (i.e., training or education) in understanding and predicting those differences. In most cases, both nature and nurture play important roles in shaping a complex behavior. However, in the case of behavioral security, the extent of nature’s influence, compared to that of nurture, is largely unknown from the literature.

The study reported here was designed on the premise that a better understanding of the roles of nature versus nurture in shaping behavioral security would help improve efforts for fraud prevention. Philosophers have long debated the role of nature (i.e., biology) versus nurture (i.e., environment) in shaping human behavior. The business research community has begun to take interest in this debate when examining user behavior in areas such as technology acceptance and media choice. From Neuro Information Systems (NeuroIS) (e.g., Dimoka et al. 2011), to physiological studies (e.g., Haney et al. 2007), and to the four drives of human nature (Abraham et al. 2009), the hunt for biological artifacts underlying cognitive processes is evidenced by a growing literature of theoretical development (Kock 2004; Kock 2009; Pirolli and Card 1999) as well as empirical investigations. However, although empirical methodologies based on physiological or neurological measures are an important step towards a better understanding of biological mechanisms underlying user behavior in the organizational setting, they fall short in several important areas.

First, they fail to shed light on the nature versus nurture debate. Human behavior is often conceptualized as the product of both nature and nurture. The extent to which a specific behavior or trait of the phenotype, or the collection of observable characteristics of an individual, is determined primarily by nature (i.e., the genotype), or nurture (i.e., the environment), varies and must be determined empirically. Moreover, neurological or physiological evidence offers estimates for the population, rather than explanations for individual differences. Existing approaches, such as the evolutionary psychology perspective (Kock 2009), focus on features that have evolved to be common across the population. Although understanding the population in general is important, this strategy provides little insight into those aforementioned factors that lead to differences in individual behaviors in the modern business environment. We believe it is important to understand the causes of those individual differences in the extent to which individuals have adopted desirable measures, have avoided risks, and have sensed or failed to sense an imminent risk.

Our specific research questions therefore are: To what extent is behavioral security malleable by environmental forces (e.g., managerial interventions or ethics training), compared to that which is determined by genetic makeup? For example, why are some users more cautious about the potential for security compromises than others? Why are some individuals easier prey for fraudulent scams than others? In addition, how important is the role of nurture or environment, compared to that of biology? Perhaps a more ominous question is: how much can we even expect training to help?

# Behavioral Genetics

Behavioral genetics, or the disciplinary examination of the role of genetics in animal behavior, has the potential to shed light on the pronounced individual differences in behavioral security. The field of behavioral genetics commonly uses the twin study method to separate genetic factors from environmental components. By comparing identical versus fraternal twins, one can calculate the extent to which a certain behavioral trait (e.g., response to a fraudulent scam) is determined by genetic or environmental influences. This methodology is gaining momentum in business research, as scholars report the extent of genetic influences across multiple disciplines, ranging from consumer behavior (Hirschman and Stern 2001), consumer decision making (Simonson and Sela 2011), entrepreneurship (Nicolaou et al. 2008a; Nicolaou et al. 2008b; Shane et al. 2010), financial risk-taking (Cesarini et al. 2008; Cesarini et al. 2010), bargaining (Wallace et al. 2007), political partisan attachment (Fowler and Schreiber 2008; Settle et al. 2009), and leadership (Arvey et al. 2006; Arvey et al. 2007; Chaturvedi et al. 2011; Johnson et al. 2004; Johnson et al. 1998).

Behavioral genetics as a discipline is concerned with genetic correlates of phenotype, or observable behaviors or traits. Personality (Plomin and Caspi 1999) and intelligence (Plomin and Spinath 2004) in particular have been the primary focus of intense research on human behavioral genetics. With family, adoption, and twin designs, behavioral genetics researchers estimate heritability of a behavioral trait, or the extent to which individual differences in the trait can be attributable to DNA or environmental differences in a population. The twin study design, in particular, is frequently utilized to estimate the heritability of a behavioral trait, such as behavioral security, by comparing monozygotic (MZ, or commonly known as “identical”)versus dizygotic (DZ, or commonly known as “fraternal”) twins.

Based on theories of quantitative genetics, observed traits can be conceptualized as manifestations of underlying genotypes as well as environmental forces. The relative importance of such latent factors can be inferred by comparing observed correlations among family members to their expected correlations based on the degree of shared genetics versus environments. The classical twin study design is particularly useful for estimating the influence of genotype (A), shared environment (C), and non-shared environment (E), or what is commonly referred to as the ACE model. These main sources of genetic and environmental variations considered in twin studies include:

* Genetic influences (A) represent the total effects of an individual’s genotype on the individual’s observed trait. Because MZ twins share 100% of the genotype, and DZ twins share 50% of the genotype on average, traits that are exclusively under genetic influences are expected to demonstrate expected correlations of one for MZ twins, and .5 for DZ twins.
* Shared environmental influences (C) refer to environmental factors common across the twin pair, such as parenting style, shared home environment, and shared childhood diet.
* Un-shared environmental influences (E) include different environmental circumstances unique to each of the twin members, such as different friends, classrooms, or even schools.

Decades of behavioral genetics research across different cultures have consistently shown heritability estimates of about .5 for both personality (Plomin and Caspi 1999) and intelligence (Plomin and Spinath 2004). In other words, genetic differences explain about 50% of the total variance in personality or intelligence. Environmental differences, such as family environment, education programs, or work environment, contribute the other half of total variance in these two domains.

Traditionally, heritability, or the genetic effects on individual differences (A), is estimated using this standard formula (Falconer and MacKay 1996):

h2 = 2(rMZ – rDZ)

where h2 is the heritability estimate, rMZ is the MZ twin intraclass correlation, and rDZ is the DZ twin intraclass correlation. The heritability estimate h2 represents twice the difference between the correlation of identical twins versus that of fraternal twins.

The relative contribution of shared environmental effects (C) is estimated as

c2 = 2 rDZ - rMZ

The relative contribution of non-shared environmental effects (E) is estimated as

e2 = 1 - h2 + c2

When multiple variables, including control variables, are considered simultaneously, a biometric model based on Structural Equation Modeling (SEM) is most often conducted to estimate the relative contributions of A, C and E to twin resemblance (Neale and Cardon 1992); we apply this approach to behavioral security. The standard SEM model is illustrated in Figure 1. Observed behavioral security measures are represented by the rectangular shapes of Twin 1 and Twin 2. These observations are theorized to reflect influences of the three latent factors A, C, and E, which are represented by the circle shapes. A1, C1, E1, A2, C2, and E2 illustrate the three latent factors of the ACE model for twins 1 and 2. The regression coefficients of the observations on the latent factors are represented by lowercase letters: a1 and a2 illustrate the additive genetic effects, c1 and c2 the shared environmental effects, and e1 and e2 the unshared environmental effects. These coefficient estimates would shed light on the genetic basis of behavioral security. If behavioral security is completely genetically determined, then coefficients a1 and a2 would be 1.0. In contrast, if behavioral security is completely driven by environmental influences, then coefficients a1 and a2 would be zero. Because MZ twins share 100% of the same genes, covariance between the two MZ twins for latent component A is set to 1. In contrast, DZ twins share 50% of their genes on average, hence such covariance between the DZ twins for latent component A is set to .5. Because both MZ and DZ twins share the same common environment within the twin pair, the covariance for the latent component E is set to 1 for both MZ and DZ twins. Non-shared environment component E is by definition unshared between the twin siblings, and therefore zero covariance is assumed for both MZ and DZ twins.

**Figure 1. Path Model for Behavioral Security for Twins 1 and 2.**

Twin 1

a1

c1

e1

Twin 2

a2

c2

e2

MZ = 1; DZ = 1

MZ = 1; DZ = .5

|  |
| --- |
|  |

# Nature vs. Nurture: The Case of Behavioral security

Here we explain how the twin design, a classic behavioral genetics research method, can be applied to understand the role of nature versus nurture in the vulnerability for behavioral security. Recent studies on fraud prevention behavior, such as resistance to impulsive clicking on fraudulent messages (e.g., Galletta et al. 2011), reveal that, even after years of publicizing the need for making backups and avoiding clicking on fraudulent messages, users often fail to heed the warnings. Many users also continue to click through to websites that are likely to be hostile, even when they have generic subject headers and generic text, and even if they are from strangers and have numeric URL links to content. Furthermore, some users are especially prone to believe outrageous claims of winnings, commissions for transferring large sums of money, or inheritances from unknown decedents. Therefore, we need more than simple behavioral or experimental models to more fully understand the dynamics of behavioral security.

Common across twin studies in business research is the finding that genetic determinants explain a significant portion of individual differences in prudence (Simonson and Sela 2011), risk taking (Cesarini et al. 2010) and cooperative behavior (Cesarini et al. 2008). Moreover, molecular genetics research has identified allelic correlates of personality traits such as novelty seeking (Cloninger et al. 1996). Because these traits may underlie many of the behavioral issues in security, we anticipate genes to play a considerable role in explaining why some individuals are more prone to experience than others.

Preliminary findings from the limited literature on fraud suggest the presence of personality correlates of behavioral security. In an experimental study, Galletta et. al. (2011) found that specific personality traits, such as financial risk propensity, distrusting stance, and the ability to focus, partially predicted the user’s propensity to click on fraudulent messages. Heritability of financial risk propensity, and other financial decision making behaviors, has been estimated to be around .25 (Cesarini et al. 2010). In other words, 25% of individual differences can be attributed to genetic variations. The rest can be attributed to nurture, or variations in the environment where these individuals have developed. Distrusting stance is likely to be a subset of the agreeableness dimension, whereas the ability to focus can be a manifestation of the conscientiousness dimension, of the Big-Five Personality theory (Norman, 1963). As indicated earlier, heritability estimates for personality dimensions are reported to be consistently around 50% in the literature (Plomin and Caspi 1999). These findings give strong reason to suspect that individual differences in propensity to engage in secure behavior can be at least partially due to genetic differences.

Empirical literatures from behavioral security, psychology, and behavioral genetics allude to potential genetic basis for behavioral security for two theoretical reasons: Risk taking, and decision biases. The roles of these two concepts in behavioral security, and their genetic bases, are discussed here.

## Risk Taking

Common across twin studies in business research is the finding that genetic determinants explain a significant portion of individual differences in prudence (Simonson and Sela 2011) and risk taking (Cesarini et al. 2010). Moreover, molecular genetics research has identified allelic correlates of personality traits such as novelty seeking (Cloninger et al. 1996), sometimes known as sensation seeking. Sensation seeking is an important mediator in the genetic effects on entrepreneurship. Entrepreneurship, or the propensity to start one’s own business, is a relatively heritable trait, and the sensation seeking dimension of personality accounts for a significant portion of variation in entrepreneurship. Heritability of financial risk propensity, and other financial decision making behaviors, has been estimated to be around .25 (Cesarini et al. 2010). In other words, 25% of individual differences can be attributed to genetic variations. The rest can be attributed to nurture, or variations in the environment where these individuals have developed. Financial risk taking behaviors, such as playing bridge with large wagers, or financial gambling, are known to correlate with variation in the dopamine system at the genetic level (Dreber et al. 2011).

These findings suggest that the propensity to take risks, seek novelty, or pursue sensation is heritable to some extent, and the trait manifests itself across several domains of behavior in the business context. Because financial risk propensity is one of the few personality factors that predicted the user’s propensity to click on a fraudulent message (Galletta et al. 2011), these findings suggest that individual differences in behavioral security can be at least partially attributable to genetic differences.

## Decision Biases

The behavioral security literature highlights the role of decision biases, such as framing and anchoring, in explaining why consumers or investors fall for fraudulent claims (Consumer\_Fraud\_Research\_Group 2006; Kirlappos and Sasse 2012; Office\_of\_Fair\_Trading 2009). Framing, in particular, is one of the decision making biases that correlate with cognitive ability (Stanovich and West 2008), which is highly heritable (Plomin and Spinath 2004). Vulnerability to the framing effect as a decision making bias was recently found to have a genetic basis (Roiser et al. 2009). Specifically, genetic variation at the Serotonin transporter-linked polymorphic region (5-HTTLPR) is associated with individual differences in the degree to which their behaviors are influenced by the framing effect. Specifically, this genetic variation is correlated with the level of amygdala reactivity, which affects decision making biases driven by contextual cues and uncertainty (Roiser et al. 2009). The amygdala plays a critical role in regulating dopamine levels, which influence decision making and choices (Rogers 2011). Therefore, these empirical studies suggest that there might be a genetic basis for decision biases that make individuals susceptible to fraudulent schemes.

Beyond studying the phenotype, the behavioral security literature has focused largely on the nurture side of the nature-nurture debate. The role of nature, in contrast, has not been examined, to the best knowledge of the authors. A number of studies have evaluated the effectiveness of training programs for fraud prevention and security. Fear appeals (Boss and Galletta 2008), anti-fraud educational websites (Sheng et al. 2010), PhishGuru, a specialized training program (Kumaraguru et al. 2009), and “Solid” training (Kirlappos and Sasse 2012) have all shown low to moderate impact on safety practices.

These findings suggest that both nature and nurture could play significant roles in shaping behavioral security. By employing the classic twin design of behavioral genetics research, this study will uncover the relative contribution of genetic makeup versus environmental factors to individual differences in behavioral security.

# Research Methodology

The empirical data collection efforts involved participant enrollment, questionnaire data collection, and a behavioral security test, described below, at the annual Twins Days festival in Twinsburg, Ohio, in summer 2012. According to the official website, the Twins Days festival is the largest annual gathering for twins and other multiples in the world. This annual event routinely attracts more than 2,000 pairs of twins who have opportunities to participate in research studies like this one, in addition to social events. Behavioral genetic researchers have frequently collected research data at the festival (e.g., Ashenfelter and Krueger 1994; Settle et al. 2009; Wise et al. 2007).

## Participants

Four hundred and ninety-seven participants participated in this research study. Zygosity data were missing from five pairs of twins, and data from the twin sibling were missing from three participants. The final dataset included a total of 242 pairs of twins, which consisted of 144 pairs of MZ twins, and 98 pairs of same-sex DZ twins, resulting in an effective sample size of 392 participants. The participants’ ages ranged from 18 to 80, with an average of 33.5, and a median of 27. Sixty (12.20%) participants reported having been fraud victims.

One method of ensuring that MZ and DZ twins were drawn from comparable populations is to examine the distributions of relevant demographic measures between the two groups. If there are any significant differences between the MZ and DZ twins, we would then include the relevant variables in subsequent SEM analysis as covariates. Summary statistics in Table 1 illustrate that the MZ and DZ twin participants are comparable in terms of age and gender. They are also comparable in terms of Facebook account ownership, one key indicator of online experience, and whether they have been fraud victims. Inferential statistics suggest no significant differences along any of these dimensions between the two twin groups. Thus, while the same size is relatively small, especially for DZ twins, there appears to be no systematic bias in the sample that would compromise the resulting estimates of the SEM analysis.

**Table 1. Comparative Statistics of MZ versus DZ Twin Participants**

|  |  |  |  |
| --- | --- | --- | --- |
|  | MZ twins (N = 288)Mean (S.D.) | DZ twins (N = 196)Mean (S.D.) | Inferential Statistics |
| Age (in years) | 34.47 (17.17) | 29.66 (13.85) | *t*(376) = 1.815, *p* = .07 |
| Female | 208 (71.2%) | 150 (79.8%) | *X*2 (1) = .895, *p* = .34 |
| Facebook account ownership | 208 (71.2%) | 85 (81%) | *X*2 (1) = .00, *p* = .99 |
| Been a fraud victim | 42 (14.6%) | 18 (9.2%) | *X*2 (1) = 3.131, *p* = .08 |

## Design

Zygosity (i.e., whether the twins are MZ or DZ) as a dichotomy factor is the primary independent variable and is measured with the question “Is your twin brother/sister an identical twin? That is, are you monozygotic twins?” (Ashenfelter and Krueger 1994). Self-report measures of zygosity have been shown to correlate nearly perfectly with genetic verification (Wise et al. 2007). Therefore, this self-report item should be sufficient for measuring zygosity for the purpose of this study. Demographic information, such as gender, age, education, occupation, and estimated family income levels (based on zipcode), were also collected as potential control variables.

The dependent variable in this study is the participant’s performance on eight questions in the behavioral security test discussed below.

## Materials

In addition to demographic measures, the behavioral security test constitutes the primary materials for measuring the dependent variable in the current study. The behavioral security test, based on a modified version of the SonicWALL Phishing IQ Test[[2]](#footnote-2), includes four items designed to simulate online deception tactics commonly seen in either consumer or business environments. The four simulated fraud messages or webpages included: IRS, World of WarCraft, BNY Mellon, and PayPal. Similar items have been used in prior fraud studies (e.g., Galletta et al. 2011; Jagatic et al. 2007; Sheng et al. 2010). The test also includes three legitimate login-pages (i.e., J.P Morgan, Ernst & Young, and eBay), and one legitimate Wells Fargo email notification.

All four phishing-simulation items can be considered as the mimicking tactic according to the Theory of Deception (Johnson et al. 2001). Mimicking as a relatively common online deception tactic (Grazioli and Jarvenpaa 2003) presents the potential victim with information that misleads (Johnson et al. 2001).

***Procedure***

As described earlier, the study involved participant enrollment at the Twins Days Festival. After providing consent, participants answered a questionnaire regarding their behavioral security experience, Internet technology usage, and personality assessments. The questionnaire also included the eight-question behavioral security test. The participant was shown printed copies of e-mail messages or webpages used in this behavioral security test and was asked to determine if each of them was legitimate or fraudulent. The participant responded to all stimuli on site. Both twins in a pair must agree to participate in order to join this study. Each participant received $10 in compensation for participation, but only after both participants had completed the study.

# Results

Performance on the behavioral security test is summarized in Table 2. Because there were eight questions on the test, the highest possible score for each participant is 8. The MZ and DZ twins performed at comparable levels. There was no statistically significant difference between the two groups.

**Table 2. Total Scores (Out of 8) on the Behavioral security Test**

|  |  |  |  |
| --- | --- | --- | --- |
|  | MZ twins (N = 292) | DZ twins (N = 188) | *Inferential Statistics* |
| Total Score (range: 0 - 8) | 4.87 (1.20) | 4.23 (1.10) | *t*(479) = .139, *p* = .49 |

To evaluate the heritability of performance on the behavioral security test, a series of behavioral genetic analyses were performed. First, consistent with the classic literature on behavioral genetics, a simple comparison of intra-class correlation was performed as a first test of the rate of twin concordance in behavior (Alford, Funk, and Hibbing 2005; Settle et al 2009). Our analysis reveals that the intra-class correlation is different for MZ twins (.58) and DZ twins (.36) (see Table 3). As heritability can be estimated as twice the difference between the MD and DZ correlations, the h2 of the behavioral security test performance was estimated to be .44. In other words, genetic variations account for about 38 percent of the variance in behavioral security test results. Table 3 summarizes these findings.

**Table 3. Genetic and Environmental Influences on the Behavioral Security Test Total Scores, based on Intra-Class Correlations**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | Intra-class Correlation | Heritability (h2 or a2) | Shared Environment (c2) | Non-shared Environment(e2) |
| Phenotype | MZ | DZ | 2\*(MZ-DZ) | (2\*DZ)-MZ | 1-MZ |
| Total Test Score | .58 | .36 | .44 | .14 | .86 |

The next step was to examine the degree of similarity between twins within pairs using covariance-based univariate Structural Equation Modeling techniques. The method of maximum likelihood as operationalized in the OpenMx library (Boker et al. 2011) of the R statistical package was used to estimate the relative contributions of genetic effects (A), shared environmental effects (C), and unshared environmental effects (E) to twin resemblance in behavioral security test performance (Falconer and MacKay 1996; Neale and Cardon 1992) in the ACE model (see Figure 1). This technique allow us to use maximum likelihood methods to generate parameter estimates for the magnitude of the ACE components separately, along with the size of the errors of these estimate, while at the same time testing and comparing the fit of various models (Neale and Cardon 1992).

The first step is to test the full ACE model illustrated in Figure 1 using the dataset. ACE model testing is conducted using the standard approach to quantitative genetic modeling that fits the ACE structural equation model to the twin dataset. The genetic effect component A estimated in the model serves as a primary indicator of the genetic basis of behavioral security. If differences in behavioral security measures are completely determined by genetic variation, then the estimate for the genetic effect component would be one. Conversely, if behavioral security as a phenotype is driven entirely by environmental factors, then the estimate for component A would be zero. Components A, C, and E, as well as the path coefficients are estimated by analyses of variance and covariance components within twin pairs. The fit of the overall ACE model is assessed based on Log Likelihood and the Akaiki information criterion (AIC) (Akaike 1987).

Table 4 summarizes fit results for the full ACE model, and two submodels: CE, and AE. The -2 Log Likelihood (i.e., -2LL) value and the Akaike information criterion (AIC) (Akaike 1987) revealed that the best fitting model for explaining individual differences in behavioral security test performance included A,C and E. The two submodels – CE and AE, both lacking the genetic influence component A, are significantly inferior to the full ACE model (*p* < .001 in both cases). The modeling results indicate that 27.65% of the variance in the dependent measure is explained by genetic differences. 36.44% of the variance can be attributed to shared environments, whereas 39.13% can be attributed to non-shared environments.

**Table 4. ACE Model Comparisons: Behavioral Security Test Performance**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Model | A  | C  | E  | -2 LL | AIC | *df* | *p* |
| ACE | 27.65% | 36.44% | 39.13% | 1339.315 | 501.3146 | *419* | *--* |
| AE | 44.55% | -- | 55.45% | 1340.443 | 500.4431 | *420* | *< 0.001* |
| E |  | -- | 92.88% | 1354.885 | 512.8854 | *421* | *< 0.001* |

To summarize, both intra-class correlations and ACE modeling reveal that variations in performance on the behavioral security test are partially explained by variations in genetic makeup.

# Discussion

This study was designed to shed light on the extent to which behavioral security is malleable by environmental forces (e.g., managerial interventions or ethics training), compared to that which is determined by genetic makeup. We found that heritability plays a role in behavioral security, accounting for 44% of the variance in performance on a behavioral security test. Our findings, although preliminary in their current form, indicate that individual differences in at least certain measures of behavioral security are substantially explained by genetic influences. Future research should address the types of security risks that provide for heritable victimization. The victimization test addressed different types of phishing messages and sites, while the behavioral measure represented only a “mimicking” scam.

Distinguishing biological from environmental antecedents provides implications for researchers and practitioners alike. First of all, the focus on explaining sources of individual differences makes a significant contribution theoretically by advancing existing research on the biological basis of victim behavior using the perspectives of evolutionary psychology and psychophysiology. Conceptual distinctions of behavioral genetics from these existing perspectives are discussed below. These theoretical distinctions are relevant not just for behavioral security research, but also organizational research in general. Theoretical comparisons are then followed by a discussion of specific implications for research and managerial practices.

## Behavioral Genetics vs. Evolutionary Psychology

Evolutionary psychology, a theoretical approach that seeks to explain human behavior from an evolutionary view (Kock 2004; Kock 2009; Pirolli and Card 1999), represents an important approach that can be used to understand the biological basis of fraud victim behavior. Human evolution has generally been a slow process over thousands of years. In contrast, widespread adoption of information technology did not take place until less than twenty years ago. Potential fraud victims who act as business users must adapt to and perform in the modern technology environment with skills and traits that have survived the historical process of evolution. Evolutionary psychologists argue that such skills and traits as attention to colors (Kock 2009), tendency for predators to minimize time spent handling prey (Hantula et al. 2008), or natural drives to acquire, bond, comprehend and defend (Abraham et al. 2009), have evolved to help humans survive in a hunter/gatherer society, as opposed to the modern technology environment. Understanding the evolutionary roots of human behavior provides insight as to why certain technology features work more effectively than others for the human user. For example, evolutionary theory has been used to explain why purchasing volume is an inverse function of website delay duration (Hantula et al. 2008).

Behavioral genetics and evolutionary psychology share a few major assumptions. First, both disciplines emphasize the role of biological roots in human behavior. Both approaches assume the existence of genotype, or the genetic correlates, that are responsible for the development of the phenotype, or observable characteristics, of an individual. Second, both disciplines also recognize the significant role of environment in shaping the phenotype. The relationship between genotype and phenotype can be expressed as:

genotype (G) + environment (E) 🡪 phenotype (P)

Behavioral genetics differs from evolutionary psychology, however, in terms of the researcher’s objectives. Evolutionary psychologists search for human universals (e.g., attention to colors, as discussed by Kock 2009), traits that are common across the population because of their survival value during the Stone Age. These traits are present in modern humans because they helped our ancestors survive challenges present in the ancient environment. In other words, the approaches posit that the phenotype we observe today is a product of genetic selection in response to changing and challenging environmental factors.

Behavioral geneticists, on the other hand, seek to explain differences among individuals, rather than traits that are universal across the entire human population. For example, with the phenotype attention to colors, behavioral geneticists are interested in the reasons why some individuals have better attention to colors than others, despite the general tendency for all seeing individuals to attend to colors. While evolutionary psychologists seek common phenotype that has evolved through a common genetic selection process in response to common environmental threats, behavioral geneticists look for differences in phenotype that can be explained by differences in genotype or environment. As such, the behavioral genetics field complements the evolutionary psychology perspective in a theoretically significant fashion.

Most importantly, behavioral genetics research sheds light on the nature versus nurture debate. To what extent is a fraud victim’s behavior determined by genetic makeup? How malleable is behavioral security by environmental forces, such as corporate training? While evolutionary psychology recognizes the interaction between universal traits with the modern work environment, only behavioral genetics research can provide precise measures of heritability, the extent to which a behavioral trait is determined by genetic makeup.

## Behavioral Genetics vs. Psychophysiology

Psychophysiology, the examination of the physiological basis of human behavior, is another important approach to understand the biological basis of behavior in the domain of systems use, which we are extending to include behavioral security. NeuroIS maps out the neurological basis of such behavior (Dimoka et al. 2011), whereas galvanic skin response (e.g., Haney et al. 2007), heart rate, and pupil dilation (Sheng and Joginapelly 2012), among others, have been adopted as objective measures of performance or emotional responses. Similar to behavioral geneticists and evolutionary psychologists, psychophysiologists believe the understanding of biological basis of user behavior provides theoretical and empirical insight that cannot be obtained through behavioral considerations alone.

Nevertheless, behavioral genetics differs from the psychophysiological approach in several ways. First, as discussed earlier, behavioral genetics is concerned with finding sources of individual differences, rather than commonalities. Psychophysiology, in contrast, focuses on identifying physiological mechanisms underlying behavioral traits that are common across the population. For example, the Neuro IS research program specifies brain regions that tend to activate during an Information Systems (IS) task across multiple IS users (Dimoka et al. 2011). Different brain regions may be responsible for different user behaviors, but the regions are believed to be relatively similar across individuals. Behavioral genetics, on the other hand, would help IS researchers understand why different individuals fall victim to fraud at different rates of likelihood. Comparisons of brain images of identical twins versus their same-sex siblings reveal individual differences in brain activities that are attributable to genetic differences. These activities are positive in some individuals, and negative in others, resulting sometimes in an overall non-active region at an aggregate level, even though the region is active at the individual level (Koten et al. 2009). This finding suggests that behavioral security research can benefit both theoretically and empirically by considering behavioral genetics in conjunction with cognitive neuroscience approaches.

Moreover, psychophysiology focuses exclusively on describing the phenotype. Neurological activities, heart rate variability, skin conductance or other physiological responses are all expressions of an individual’s phenotype. Understanding and measuring the phenotype is an important task, as organizational scholars have done for decades with behavioral or perceptual measures. However, the observation of the phenotype alone tells us little about how genetic or environmental forces lead to the phenotype we observe. For example, Dimoka et al. (2011) locates brain regions that are activated when the user trusts a system. While an important finding itself, the discovery raises the question as to the extent to which differences in the trusting behavior, and the associated physiological responses, are due to differences in genetic makeup as opposed to environmental factors. The linkage between genetics and brain morphology is more than a straightforward one-to-one relationship (Hariri et al. 2002). The brain, as well as human behavior in general, develops often as a consequence of genetics expressed in reaction to environmental influences. In other words, examining physiology alone sheds little light on the nature versus nurture debate.

To summarize, behavioral genetics provides a distinctively unique approach to understand the biological roots of behavioral security. Building upon evolutionary psychology and psychophysiological research, behavioral genetics studies will enrich our research by estimating the relative power of nature versus nurture in influencing victimization.

## Implications for Research

Results of this study have several implications for research. First of all, findings about genetic influences may suggest stability of behavioral security traits over time. Genetic manifestation is durable, and so if the genetic makeup influences at least some of the variances we see in such victimization, the unsecure or risky user behavior we observe may be more durable than normally anticipated.

Theoretical understanding of the mechanisms underlying the genetic influences could help us unpack the specific sources of such influences. Additional research should also examine factors that moderate or mediate these genetic influences, such as decision making biases, or risk taking propensity. Finally, future studies should explore multivariate models using other measures of behavioral security to triangulate the findings.

Future studies will be able to adopt the twin study technique to distinguish biological versus environmental antecedents to a host of behavioral security outcomes. For example, researchers can investigate attitudes such as optimism that might lead to clicking on site URLs that are unsafe, impatience that bars careful checking on the messages received, and even error rates, systems misuse (e.g., D'Arcy et al. 2009), and reactions to managerial interventions such as fear appeals (Boss and Galletta 2008). Using direct measures of the participant’s vulnerability for behavioral security such as the participant’s response to a simulated security attack sent to the email address that the participant provided can also a potential avenue of exploration. These are but a few of the potential breakthroughs that a twin study can afford.

Future studies can build upon this simple twin design in several ways. First, genotype interacts with the environment in complex ways, and this interaction can only be modeled using more complex designs beyond the simple twin comparison method. Second, nuances of the environmental component can be further modeled using family studies. Finally, different types of actual phishing measures should be investigated to see which represent heritable discrimination and which do not. While a “mimicking” style of phishing message seems to have more of an environmental basis, studies are needed to determine whether other types have more of a genetic basis.

## Implications for Practice

One implication of our findings is that the previous emphasis on security education or training found in the literature may need to be reconsidered. Notions that behavioral security weaknesses can be resolved through education or training alone may be problematic without also taking into consideration the genetic basis of unsecure behavior. For example, Google’s “Good to Know” site cautions individual and corporate users to (1) practice strong password creation and frequent change, (2) enable 2-step verification, (3) frequently update operating systems and software, (4) beware of phishing, and (5) install and update commercial and reputable antivirus software. In addition, to the extent that some data are only stored on a user’s disk rather than all in the cloud, we believe that users should (6) make frequent backups. In spite of the growing and frequent warnings, many users just do not seem to internalize these useful tips. This study aims to determine if such behaviors are fundamentally characteristics of some genetic trait or if those behaviors are malleable and can be improved based on training, experience, or corporate edict. By knowing the extent to which differences in these secure behaviors are determined by genetic makeup versus environmental forces, this research can help managers specify areas where managerial intervention (i.e., one form of environmental influence) may be the most (as well as least) fruitful.

While practitioners often provide warnings and educational experiences to aid users in working more safely with information technologies, our study would provide perhaps more realistic expectations for such programs, and even serve to persuade management to deploy funds towards alternative solutions. For instance, if workers insist on sharing passwords, and do not heed warnings about that practice, management might redeploy training funds towards inexpensive fingerprint recognition devices. Also, if workers fail to make backups, software that makes network backups might be purchased instead.

Findings from twin studies will also benefit educators, or even parents, who strive to understand how to foster secure behavior online and to reduce the rate of cyberbullying or other forms of cybercrime. Twin and adoption studies have found very little influence that the shared family environment has on shaping personality or intelligence (Plomin and Caspi 1999; Plomin and Spinath 2004). These findings sent shock waves through the research community on parenting, which always theorized a strong relationship between a positive family environment with positive outcomes in personality or intelligence. Moreover, mental disorders, such as ADHD or autism, were blamed on poor parenting until behavioral genetics research provided evidence of strong heritability. The finding that these traits are highly heritable and are resistant to family influence not only challenged parenting theories, but also transformed parenting practices. Behavioral genetic findings of organizational behavior may even prove to challenge fundamental assumptions in a wide array of organizational practices beyond behavioral security.

## Limitations

Findings from the study reported here must be considered in light of several methodological limitations. First, while our overall sample size is relatively large for information research studies, the number of twin pairs is relatively small compared to standard twin studies. Moreover, while the sample size for MZ twins is reasonable, the DZ group is considerably smaller. Unequal sample sizes are rather common in published twin studies, especially those with data collected from the Twins Days Festival. This is probably because the festival events tend to attract MZ rather than DZ twins. There is principally no theoretical reason to suspect that the unequal sample sizes have compromised our analysis in any way.

Thirdly, current findings are based on a single measure of behavioral security. Estimates of multivariate ACE models would not only strengthen our understanding, they will also help us uncover mediating or moderating processes that shed light on the biological mechanisms underlying the genetic influences.

Finally, limitations inherent in the ACE model must be taken into consideration when interpreting these results. The ACE model assumes that genetics and the environment influence behavioral traits in an additive manner. Rigorous testing of this underlying assumption should be explored in the future. Additionally, while the ACE model presented here provides preliminary support for the role of genes in behavioral security, the model does not specify how genes may interact with the environment to produce the patterns of behavioral security we observe in the phenotype. Exploration mechanisms for interaction between genetics and the environment, such as epigenetics, will shed light on this potential limitation of the current research.

## Conclusion

Behavioral genetics, the study of the genetics of behavior, offer many opportunities to extend our research of behavioral security. By employing a twin design, the classic methodology of behavioral genetics research, this study is among the first to unpack the genetic versus environmental determinants of individual differences in information systems, especially with respect to security behavior. It is particularly striking that 44% of the performance on a test that requires distinguishing 8 actual sites or emails from fraudulent ones appears to be traced to genetics.

The study of genetic versus environmental influences has the potential promise to push the boundaries, and challenge the basic assumptions of many organizational theories beyond the fraud prevention literature. After all, the fraud victim is made of genetic materials, and a full understanding of genetic influences will only improve theoretical explanations for victimization behavior.

# References

Abraham, C., Junglas, I., Watson, R.T., and Boudreau, M.-C. 2009. "Studying the Role of Human Nature in Technology Acceptance," in: *International Conference on Information Systems*. Phoenix, Arizona.

Akaike, H. 1987. "Factor Analysis and Aic," *Psychometrika* (52:3), pp 317-332.

Arvey, R.D., Rotundo, M., Johnson, W., Zhang, Z., and McGue, M. 2006. "The Determinants of Leadership Role Occupancy: Genetic and Personality Factors," *The Leadership Quarterly* (17:1), pp 1-20.

Arvey, R.D., Zhang, Z., Avolio, B.J., and Krueger, R.F. 2007. "Developmental and Genetic Determinants of Leadership Role Occupancy among Women," *Journal of Applied Psychology* (92:3), pp 693-706.

Ashenfelter, O., and Krueger, A. 1994. "Estimates of the Economic Return to Schooling from a New Sample of Twins," *American Economic Review* (84:5), pp 1157-1173.

Boker, S., Neale, M.C.C.L., Maes, H., Wilde, M., Spiegel, M., Brick, T., Spies, J., Estabrook, R., Kenny, S., Bates, T., Mehta, P., and Fox, J. 2011. "Openmx: An Open Source Extended Structural Equation Modeling Framework," *Psychometrika* (76:2), pp 306-317.

Boss, S., and Galletta, D.F. 2008. "Scared Straight: An Empirical Comparison of Two Major Theoretical Models Explaining User Backups," in: *Ninth International Research Symposium on Accounting Information Systems*. Paris, France.

Cesarini, D., Dawes, C.T., Fowler, J.H., Johannesson, M., Lichtenstein, P., and Wallace, B. 2008. "Heritability of Cooperative Behavior in the Trust Game," *Proceedings - National Academy of Sciences USA* (105:10), pp 3721-4003.

Cesarini, D., Johannesson, M., Lichtenstein, P., Sandewall, Ã.r., and Wallace, B. 2010. "Genetic Variation in Financial Decision-Making," *The Journal of Finance* (65:5), pp 1725-1754.

Chaturvedi, S., Arvey, R.D., Zhang, Z., and Christoforou, P.T. 2011. "Genetic Underpinnings of Transformational Leadership: The Mediating Role of Dispositional Hope," *Journal of Leadership & Organizational Studies* (18:4), pp 469-479.

Cloninger, C.R., Adolfsson, R., and Svrakic, N.M. 1996. "Mapping Genes for Human Personality," *Nature Genetics* (12:1), pp 3-4.

Consumer\_Fraud\_Research\_Group. 2006. "Investor Fraud Study," NASD Investor Education Foundation.

D'Arcy, J.A., Hovav, A., and Galletta, D.F. 2009. "Awareness of Security Countermeasures and Its Impact on Information Systems Misuse: A Deterrence Approach," *Information Systems Research* (20:1), pp 79-98.

Dimoka, A., Pavlou, P.A., and Davis, F. 2011. "Neurois: The Potential of Cognitive Neuroscience for Information Systems Research," *Information Systems Research* (22:4), pp 687-702.

Dreber, A., Rand, D.G., Wernerfelt, N., Garcia, J.R., Vilar, M.G., Lum, K., and Zeckhauser, R. 2011. "Dopamine and Risk Choices in Different Domains: Findings among Serious Tournament Bridge Players," *Journal of Risk and Uncertainty* (43:1), pp 19-38.

Falconer, D., and MacKay, T. 1996. *Introduction to Quantitative Genetics*. Essex UK: Longmans Green.

Fowler, J.H., and Schreiber, D. 2008. "Biology, Politics, and the Emerging Science of Human Nature," *Science* (322:5903), pp 912-914.

Galletta, D.F., Moody, G., Dunn, B.K., and Walker, J. 2011. "Which Phish Get Caught? An Exploratory Study of Individual Susceptibility to Phishing," *International Conference on Information Systems*, Shanghai, China.

Grazioli, S., and Jarvenpaa, S.L. 2003. "Deceived: Under Target Online," *Communications of the ACM* (46:12), pp 196-205.

Haney, M., Pike, J., Galletta, D., Polak, P., and Chung, T.R. 2007. "Does Our Web Site Stress You Out? Information Foraging and the Psychophysiology of Online Navigation," *ICIS 2007 Proceedings*).

Hantula, D.A., Brockman, D.D., and Smith, C.L. 2008. "Online Shopping as Foraging: The Effects of Increasing Delays on Purchasing and Patch Residence," *Professional Communication, IEEE Transactions on* (51:2), pp 147-154.

Hariri, A.R., Mattay, V.S., Tessitore, A., Kolachana, B., Fera, F., Goldman, D., Egan, M.F., and Weinberger, D.R. 2002. "Serotonin Transporter Genetic Variation and the Response of the Human Amygdala," *Science* (297:5580), pp 400-403

Herley. 2009. "So Long, and No Thanks for the Externalities: The Rational Rejection of Security Advice by Users," *the 2009 workshop on New security paradigms workshop* Oxford, United Kingdom.

Hirschman, E., and Stern, B. 2001. "Do Consumers' Genes Influence Their Behavior? Findings on Novelty Seeking and Compulsive Consumption," *Advances in Consumer Research* (28), pp 403-410.

Jagatic, T.N., Johnson, N.A., Jakobsson, M., and Menczer, F. 2007. "Social Phishing," *Communications of the ACM* (50:10), pp 94-100.

Johnson, A.M., Vernon, P.A., Harris, J.A., and Jang, K.L. 2004. "A Behavior Genetic Investigation of the Relationship between Leadership and Personality," *Twin Research* (7:1), pp 27-32.

Johnson, A.M., Vernon, P.A., McCarthy, J.M., Molson, M., Harris, J.A., and Jang, K.L. 1998. "Nature Vs Nurture: Are Leaders Born or Made? A Behavior Genetic Investigation of Leadership Style," *Twin Research* (1:4), pp 216-223.

Johnson, P.E., Grazioli, S., Jamal, K., and Berryman, G. 2001. "Detecting Deception: Adversarial Problem Solving in a Low Base Rate World," *Cognitive Science* (25:3), pp 355–392.

Kirlappos, I., and Sasse, M.A. 2012. "Security Education against Phishing: A Model Proposal for a Major Rethink," *IEEE Security & Privacy* (10:2), pp 24-32.

Kock, N. 2004. "The Psychobiological Model: Towards a New Theory of Computer-Mediated Communication Based on Darwinian Evolution," *Organization Science* (15:3), pp 327-348.

Kock, N. 2009. "Information Systems Theorizing Based on Evolutionary Psychology: An Interdisciplinary Review and Theory Integration Framework," *Management Information Systems Quarterly* (33:2), pp 395-418.

Koten, J.W.J., Wood, G., Hagoort, P., Goebel, R., Propping, P., Willmes, K., and Boomsma, D.I. 2009. "Genetic Contribution to Variation in Cognitive Function: An Fmri Study in Twins," *Science* (323:5922 ), pp 1737-1740

Kumaraguru, P., Sheng, S., Acquisti, A., Cranor, L.F., and Hong, J. 2009. "Teaching Johnny Not to Fall for Phish," *ACM Transactions on Internet Technology* (10:2), pp 1-31.

Neale, M.C.C.L., and Cardon, L.R. 1992. *Methodology for Genetic Studies of Twins and Families*. Kluwer Academic Publishers.

Nicolaou, N., Nicolaou, N., Shane, S., Cherkas, L., and Spector, T.D. 2008a. "The Influence of Sensation Seeking in the Heritability of Entrepreneurship," *Strategic Entrepreneurship Journal* (2:1), pp 7-21.

Nicolaou, N., Shane, S., Cherkas, L., Hunkin, J., and Spector, T.D. 2008b. "Is the Tendency to Engage in Entrepreneurship Genetic?," *Management Science* (54:1), pp 167-179.

Office\_of\_Fair\_Trading. 2009. "The Psychology of Scams: Provoking and Committing Errors of Judgment," O.o.F. Trading (ed.). United Kingdom: Office of Fair Trading.

Pirolli, P., and Card, S. 1999. "Information Foraging," *Psychological Review* (106:4), pp 643-675.

Plomin, R., and Caspi, A. 1999. "Behavioral Genetics and Personality," in: *Handbook of Personality: Theory and Research,* L.A. Pervin and O.P. John (eds.). New York, NY: Guilford Press, pp. 251-276.

Plomin, R., and Spinath, F.M. 2004. "Intelligence: Genetics, Genes, and Genomics," *Journal of Personality and Social Psychology* (86:1), pp 112-129.

Ponemon\_Institute. 2013. "2013 Cost of Data Breach Study: Global Analysis."

Potter, C., and Waterfall, G. 2012. "Information Security Breaches Survey," PricewaterhouseCoopers.

Rogers, R. 2011. "The Roles of Dopamine and Serotonin in Decision Making: Evidence from Pharmacological Experiments in Humans," *Nerupsychopharmacology* (36), pp 114-132.

Roiser, J.P., de Martino, B., Tan, G.C.Y., Kumaran, D., Seymour, B., Wood, N.W., and Dolan, R.J. 2009. "A Genetically Mediated Bias in Decision Making Driven by Failure of Amygdala Control," *Journal of Neoroscience* (29:18), pp 5985-5991.

Settle, J.E., Dawes, C.T., and Fowler, J.H. 2009. "The Heritability of Partisan Attachment," *Political Research Quarterly* (62:3), pp 601-613

Shane, S., Nicolaou, N., Cherkas, L., and Spector, T.D. 2010. "Genetics, the Big Five, and the Tendency to Be Self-Employed," *Journal of Applied Psychology* (95:6), pp 1154-1162.

Sheng, H., and Joginapelly, T. 2012. "Effects of Web Atmospheric Cues on Users' Emotional Responses in E-Commerce," *AIS Transactions on Human-Computer Interaction* (4:1), pp 1-24.

Sheng, S., Holbrook, M., Kumaraguru, P., Cranor, L.F., and J., D. 2010. "Who Falls for Phish?: A Demographic Analysis of Phishing Susceptibility and Effectiveness of Interventions," *the 28th international conference on Human factors in computing systems* Atlanta, GA.

Simonson, I., and Sela, A. 2011. "On the Heritability of Consumer Decision Making: An Exploratory Approach for Studying Genetic Effects on Judgment and Choice," *Journal of Consumer Research* (37:6), pp 951-966.

Stanovich, K.E., and West, R.F. 2008. "On the Relative Independence of Thinking Biases and Cognitive Ability," *Journal of Personality and Social Psychology* (94:4), pp 672-695.

Titus, R.M., Heinzelmann, F., and Boyle, J.M. 1995. "Victimization of Persons by Fraud," *Crime & Delinquency* (41:1), pp 54-72.

Wallace, B.r., Cesarini, D., Lichtenstein, P., and Johannesson, M. 2007. "Heritability of Ultimatum Game Responder Behavior," *Proceedings of the National Academy of Sciences* (104:40), pp 15631-15634.

Weirich, D. 2006. "Persuasive Password Security," in: *Department of Computer Science*. London, UK: University College London.

Wise, P.M., Hansen, J.L., Reed, D.R., and Breslin, P.A.S. 2007. "Twin Study of the Heritability of Recognition Thresholds for Sour and Salty Taste," *Chemical senses* (32:8), pp 749-754.

1. For details of the news story please visit http://www.webpronews.com/grocery-store-falls-for-10-million-phishing-scam-2007-10 [↑](#footnote-ref-1)
2. Available at http://www.sonicwall.com/furl/phishing/ [↑](#footnote-ref-2)