Accepted Manuscript

"This is the Way 'I' Create My Passwords..." Does the Endowment Effect Deter People from Changing the Way they Create their Passwords?

Karen Renaud, Robert Otondo, Merrill Warkentin

PII: S0167-4048(18)30909-X
DOI: https://doi.org/10.1016/j.cose.2018.12.018
Reference: COSE 1452

To appear in: *Computers & Security*

Received date: 14 August 2018
Revised date: 28 December 2018
Accepted date: 31 December 2018

Please cite this article as: Karen Renaud, Robert Otondo, Merrill Warkentin, "This is the Way 'I' Create My Passwords..." Does the Endowment Effect Deter People from Changing the Way they Create their Passwords?, *Computers & Security* (2019), doi: https://doi.org/10.1016/j.cose.2018.12.018

"This is the Way 'I' Create My Passwords ..." Does the Endowment Effect Deter People from Changing the Way they Create their Passwords?

Karen Renaud[1], Robert Otondo[2], Merrill Warkentin[2]

[1]Abertay University, Dundee; University of South Africa

[2] Mississippi State University

Abstract

The endowment effect is the term used to describe a phenomenon that manifests as a reluctance to relinquish owned artifacts, even when a viable or better substitute is offered. It has been confirmed by multiple studies when it comes to ownership of physical artifacts. If computer users also "own", and are attached to, their personal security routines, such feelings could conceivably activate the same endowment effect. This would, in turn, lead to their over-estimating the "value" of their existing routines, in terms of the protection they afford, and the risks they mitigate. They might well, as a consequence, not countenance any efforts to persuade them to adopt a more secure routine, because their comparison of pre-existing and proposed new routine is skewed by the activation of the endowment effect.

In this paper, we report on an investigation into the possibility that the endowment effect activates when people adopt personal password creation routines. We did indeed find evidence that the endowment effect is likely to be triggered in this context. This constitutes one explanation for the failure of many security awareness drives to improve password strength. We conclude by suggesting directions for future research to confirm our findings, and to investigate the activation of the effect for other security routines.

Keywords: Password Creation Routines; Endowment Effect; Change Willingness; Psychological Ownership; Scenario-Based Survey

1 Introduction

Many security awareness and training drives are delivered with the best of intentions, and appear to be received enthusiastically by the recipients. Yet these same recipients either decline to change their regular routines, or change their behavior in the short term and then revert to their original routines [169, 3]. Some trainers attribute this kind of resistance to personal failings on the part of the recipients [48, 127, 178]. This kind of attribution does not help to resolve the situation.

Researchers and organizations respond to this situation by endeavoring to improve compliance [14, 151, 177]. Resorting to compliance enhancement efforts and rule-making is understandable when organizations are concerned that employee behaviors are placing the organization's information security at risk. Some propose dealing with resistance by imposing penalties for a failure to implement mandated security measures [87, 135]. Yet these kinds of approaches can backfire, leading to resentment [17, 153], perhaps because they unacceptably erode the employee's autonomy [45].

It would be helpful to understand the underlying causes of behavioral change resistance, rather than attempting to mandate new behaviors without acknowledging the nature and complexity of the human agent [139, 60]. If we want people to change the way they behave, we should endeavor to understand exactly why they are rejecting security-related advice. We will then be in a better position to formulate interventions to minimize the impact of the core causatives that manifest as reluctance, but are due to a far more complicated interplay of multiple factors.

Humans have good reasons for their behaviors, even if they perhaps cannot, or will not, articulate them. Sometimes people are not even conscious of reasons for their own behaviors [174, 179].

The endowment effect is observed when people feel *endowed* with a particular artifact, such that they are reluctant to exchange it for any substitute, even if the substitute is superior [90]. If the endowment effect is active, and people are asked to swap "their" artifact for another, they are more reluctant than can be expected by chance [96]. This suggests that the recipient of the artifact considers their endowed artifact to be more *desirable* than the other artifact, even if both command the same price in the marketplace. Moreover, this effect can occur almost immediately the person is endowed with the artifact.

The endowment effect is usually demonstrated by showing that people over-value an endowed artifact. This is evidenced by the fact that they will require more money (WTA: will-

ingness to accept) to relinquish the endowed item than the actual value of the item i.e. what someone else would reasonably pay for it (WTP: willingness to pay) [89, 97]. They essentially *over-value* the artifact: in their eyes it is more *valuable* than the objective reality would dictate, and more valuable than an offered substitute.

There is some evidence that the endowment effect does not only apply to physical artifacts, nor that it only applies in the lab. It has also been observed being triggered by people feeling endowed with other "artifacts" such as time and intellectual property [77]. Moreover, when some effort has been expended in obtaining a particular artifact, this exacerbates the endowment effect, suggesting that effort, and not merely the object itself, contributes to the triggering of the endowment effect [119].

We wanted to find out whether people feel endowed with their personal security routines. In essence, would they be *reluctant to exchange* them for other routines, and would they *over-value* them, in terms of the protection they afford? Clark [38] talks about people "owning" solutions they have come up with to problems, and certainly finding a personal way of dealing with passwords can be thought of as a solution. Does such ownership trigger the endowment effect in the password creation context?

The endowment effect, if it is indeed activated by effort invested in coming up with routines in the information security context, probably works in concert with other factors leading to change resistance. Osman *et al.* [126] point out that successful behavioral change campaigns require a suite of interventions to be devised and deployed. They also explain that it is often challenging to predict which combination of methods will be most efficacious. A better understanding of people's rejection of security advice, and perceptions of risk, is the first step towards determining exactly which interventions are best to deploy. Here, we chose to focus on the potential influence of the endowment effect, which Arlen and Tontrup [10] consider to be a behavioral bias that can indeed be deactivated.

If we can confirm that this effect activates when it comes to security routines, proven techniques from other disciplines, where the efficacy of "muting" interventions have been confirmed [10], can be deployed to minimize its impact.

The one place where computer users encounter security risk is during authentication. The password, despite many reports predicting its imminent demise, still permeates our online lives [63]. One of the most ubiquitous pieces of advice given to computer users is to choose strong passwords that reduce the risk of not only data theft and damaged reputation, but also financial risks from ransomware attacks, loss of trust, and potential liability for damages from inadvertent hosting of Distributed Denial of Service attacks [53, 129, 172, 184]. Nonetheless,

the use of weak passwords is still prevalent [74]. We therefore chose password creation routines as the subject of our investigation. We describe a study we undertook to explore the existence and potential impact of the endowment effect in the password creation context. We report on our findings and conclude by suggesting directions for future research.

2 Reluctance to Switch

Cyber security is a relatively new phenomenon on an evolutionary scale, certainly much newer than many other areas of human risk management, such as managing physical safety or disease prevention. Due to its newness, it is thus reasonable to assume that the populace at large lacks sufficient knowledge and skills to secure their own information, systems and devices adequately [62, 138, 141, 143].

One risk mitigation technique is to enforce strength by disallowing weak passwords [154]. While this is an effective strategy, it does require installation on each and every system. The usual approach grants people the autonomy to choose a password themselves, having ensured that they know how choose to strong passwords. This strategy requires deliberate knowledge deficit-reduction efforts to be made [25, 156]. Information security researchers and practitioners consequently formulate educational and awareness drives to deliver knowledge of good practice. The aim is to improve security routines across the organization, thereby improving resilience and reducing risk [4, 76]. Governments also provide a great deal of advice to citizens in terms of how to practice good security hygiene [43, 73, 82, 120, 146].

Yet all these efforts do not seem to have been particularly successful in terms of reducing insecure behaviors [11, 36, 140]. Even those who do possess knowledge of "good practice" do not seem to be willing to change their usual routines [39, 94, 22]. It has become clear that an approach that relies solely on information provision is unlikely to be *sufficient* in terms of changing behavior [66, 69, 70, 88, 114]. It is interesting to note that the empirical findings by Warkentin *et al.* [176] showed that users prefer their own passwords over ones generated for them, even though the latter may be stronger.

As the field has come to realize that knowledge, on its own, is not the silver bullet in achieving behavior change, there have been attempts to manipulate the *choice architecture* to nudge people towards stronger passwords [51, 144]. While these manipulations show promise, they do not help us to understand the underlying reasons for reluctance to embrace stronger password choice routines.

Similar levels of change resistance manifest in other domains, too [30, 90, 81, 167]; security

behaviors are not unique in this respect. In this paper, we briefly review two prominent theories before introducing the explanation we investigated in our research: the endowment effect. We do not claim that other factors do not exert an influence; only that one influential factor might be the endowment effect, and that efforts to understand and minimize its impact might well reduce resistance.

Reasons for Change Resistance in Security

The literature suggests a wide range of explanations for unwillingness to switch when people do indeed have the knowledge to behave securely. These include: intransigence, a lack of understanding of the importance of the activity, ignorance of the severity of potential consequences, or just plain laziness [3, 52, 64, 83, 111, 113, 188]. Infusing the situation with moral undertones can achieve the opposite of what is intended [41], and is unlikely to help the situation.

A variety of explanations for change resistance have been suggested by the research literature. Laumer and Eckhardt [100] review a range of IS-related resistance theories, ranging from perceived threats [99] to power considerations [106] to *status quo* bias [93] and learned helplessness [109]. Many of the theories they discuss have been revealed when studying resistance within organizations, but some theories could well apply to personal security routines too.

Another possible explanation for change resistance is the fact that humans seek to copy their own past behaviors. Ariely and Norton refer to this phenomenon as *self-herding* [8]. This pattern might occur because people have a need for consistency [37], or because changing would require them to admit that the way they have been doing things up to that point was wrong, and this would somehow create a sense of cognitive dissonance [56]. If they were to agree to change the way they do things, this would constitute an admission that their previous routines were sub-optimal and might have led to negative outcomes. Sherman and Cohen [150] explain that people prefer to consider themselves responsible for producing *positive*, rather than *negative*, outcomes. They cite [71, 158, 115] to substantiate this argument. This would mean that if someone were asked to change a personal security routine and told that they had to do this because their existing routine was leading to negative outcomes (insecurity), they might well decline to countenance a change. Changing would constitute an admission of the inadequacy of their existing routines and implied responsibility for potentially negative outcomes, and people might understandably want to avoid this.

It is possible that a number of these factors come into play in this situation, and lead to rejection of switching suggestions, despite any persuasive attempts to describe the merits of the

alternative routine. People might even avoid listening to information that would lead to the uncomfortable feelings of dissonance. Sweeny [157] explains that people do avoid information if such information would require them to change their beliefs, take undesired actions, or be likely to elicit unpleasant emotions. All of these seem to apply to someone suggesting that a well-embedded password creation routine should be replaced.

The situation is probably multi-factorial, and complex, as is most human behavior [130]. It is likely that a range of influences come into play when people reject security advice, and that the reasons differ from person to person and from day to day, depending on a wide range of causatives, ranging from individual to contextual to organizational pressures and characteristics [20]. That being so, we cannot expect any one explanation, and intervention, to "solve" this and remove all resistance. Yet we do not have the luxury of abandoning efforts merely because the situation is so complex. We have to keep trying to pick apart all the factors leading to this resistance and reluctance. Employees can be our strongest defence against hacker attempts, but only if they behave securely. We have to find out how best to encourage and engender this kind of behavior.

In advancing explanations from non-security domains below, we make the assumption that people do indeed know what they ought to be doing (the advised routine) and how to implement it (knowledge & skills). We are not attempting to address a knowledge deficit issue in this discussion.

3 Theory Types

Markus and Robey [107] introduce two types of theories that are used when the consequences of organizational change are studied (variance and process). Burton-Jones *et al.* [31] mention both of these and add another: systems. The latter is not as applicable in our context but due consideration of process and variance theories provide a useful perspective to structure our discussion. Variance theory attempts to identify and isolate the impact of predictor variables, and their strengths, on a particular outcome. Such causal identification is generally static and snapshot based. Process theory explains how outcomes develop longitudinally i.e. in discrete and sequential stages.

Variance theories focus on factors that are necessary and sufficient conditions for contributing towards a particular outcome, such as change resistance. Process theories focus on conditions under which outcomes *can* occur, but are not guaranteed to. They focus on particular states or *stages*, and changes of such, in leading to outcomes. Table 1 provides an overview of

the key differences between these two perspectives in terms of studying resistance to change. Figure 1 contrasts the two theories.

	Variance Theory (Imperative) $\mathbf{V}_i$	**Process Theory (Emergent) $\mathbf{P}_i$**
Relationship	**V1:** Cause $\rightarrow$ Effect — Outcome $\in$ {Effect} Cause is ***necessary*** *and* ***sufficient*** Effect will **invariably** occur: — when cause is present Cause **explains** Effect	**P1:** Cause $\prec$ Effect; — Outcome $\in$ {Effect, $\emptyset$} Cause is ***necessary*** Effect may not occur — even if cause is present Cause **precedes** Effect
Amplification	**V2:** Cause++ $\rightarrow$ Effect++ Outcome $\in$ {Effect++} **More** Cause leads to **more** effect	**P2:** Cause++ $\prec$ Effect; Outcome $\in$ {Effect, $\emptyset$} Chance and random events play a role
Certainty	**V3:** Link between Cause & Effect — is **certain**	**P3:** Cause makes Effect **possible**
Trigger	**V4:** Cause leads to, and **engenders**, effect	**P4:** Effects influenced by **social phenomena**
Focus	**V5: Influential** variables taking a range of values	**P5: Discontinuous** and **emergent** phenomena
Predictability	**V6:** Outcomes are *predictable*, based on **magnitude of causative variables**	**P6:** Outcomes are *predictable* from **knowledge of process**

Legend: causes ($\rightarrow$); precedes ($\prec$); more of (++); one of ($\in$); no effect($\emptyset$)

Table 1: Contrasting Variance and Process Theories (extending Figure 3 from [107])

We cannot hope to review the behavioral change resistance field comprehensively in the related work section of a single paper, so we will provide one variance theory (habit) and one process theory (change readiness). We then introduce the endowment effect, a psychological explanation for change resistance. We will also consider whether it is a variance or process

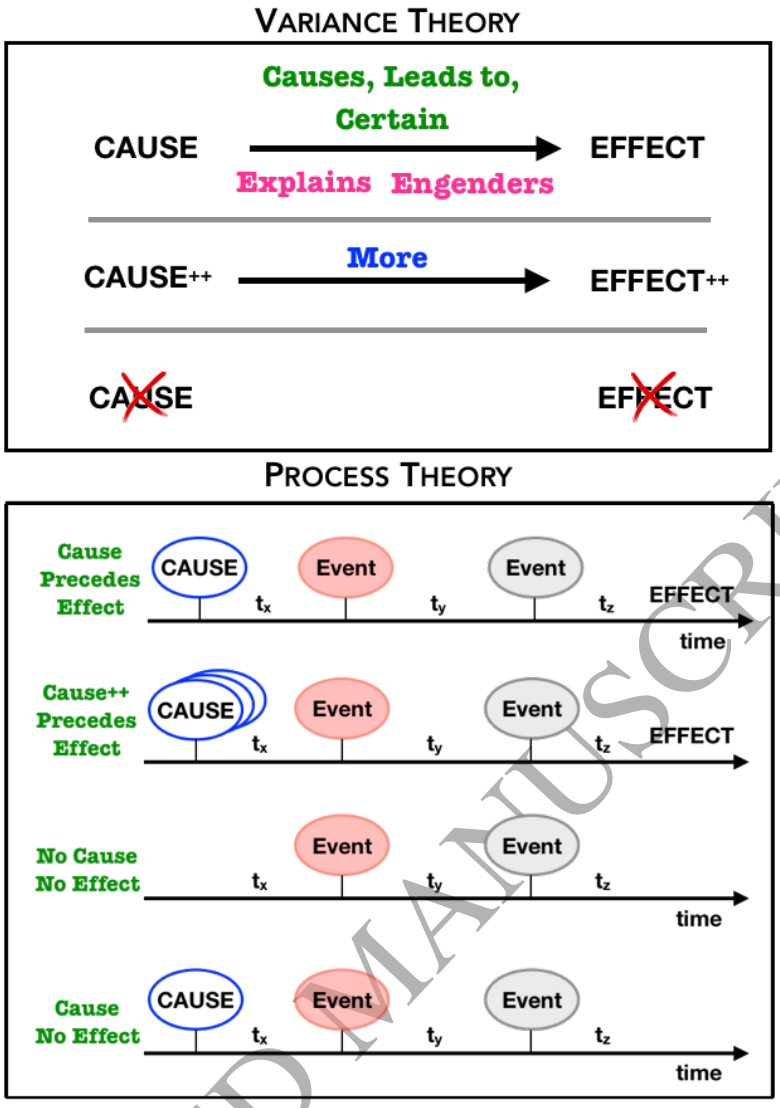

Figure 1: Top: Variance Theory (Imperative); Bottom: Process Theory (Emergent).

theory. In these discussions we will refer to instantiations of the relationships between cause and effect by number Vi (Variance) and Pi (Process), as indicated in Table 1.

To investigate the phenomenon of perceived ownership and the endowment effect, as it relates to computer users choosing, then owning, their password creation routine, we must necessarily look at both variance and process theories. Variance models provide insights into the associations that individuals perceive between various perceptions and beliefs, such as perceptions of threats and responses. Process models inform our thinking about how such perceptions and beliefs are formed over the course of time.

3.1 Habit (Variance Theory)

Binder and Boldero [20] argue that consideration of habit must be included whenever human behavior is being contemplated. James [84] argued that habits (pre-existing routines) were essential in understanding how humans behave. Aarts *et al.* [1] explain that habits develop to satisfy goals and, over time, become automatic when cued in particular situations (V1). Indeed, Bargh *et al.* [13] found that habits could be cued without people even being aware that a particular habit had been activated (V3). Indeed, Wood and Neal [182] argue that habit associations are constructed slowly as the person engages in the habitual behavior. They are not easily changed, even if current goals are altered.

Duhigg [49] explains that habitual routines are cued by context, and that they lead to a reward. As Aarts suggests, habitual behaviors become ingrained over time as the same cue repeatedly triggers the same routine (V4, V6-considering habit duration as a causative). Pinder *et al.* [131] review behavioral change publications in human-computer interaction research and find that the influence of habit is often neglected. They cite [122] to make the point that "habitual behaviors are the default behavior when people are *unable or unwilling* to make effortful decisions about how to behave" [p.3]. (Emphasis ours)

If we consider that many schools require pupils to start using passwords at a very young age, the pre-existence of password creation habits is likely in adults [104, 171], which would also contribute to their entrenchment and habitual nature (V4, V6).

Habits exhibit the characteristics of a variance theory if we consider the *cause* to be the cue ("create a password"), and the reward to be "ease of password creation", for example. Significant associations between measures of these constructs imply that the cue is sufficient to trigger activation of the habitual routine (V1). Covariance associations suggest the certain link between cause and effect, once the habit is well established, which is typical of a variance theory (V3, V6).

What many educational efforts do not acknowledge, nor factor into their delivery, is the influence exerted by such habitual pre-existing routines. When people are confronted with a new routine, and asked to switch, those familiar routines (habits) make up a powerful incentive to eschew change. Change being effortful [65], and humans being maximally efficient [52, 190], means that they are not actually making a choice between equivalent options. They are being asked to switch to a much more inefficient option, at least in the short term. Consumer behavior research terms this phenomenon "switching cost."

Humans are present-focused and more likely to be influenced by present effort than future

benefit [27], making a switch unlikely. This has been termed *psychological distance in the temporal dimension* by the construal-level theory (CLT). It rests on the core tenet that people have direct experience only of the *here and now* and create mental simulations abstracted from this experience, namely "construals", to represent objects and events that are not directly accessible through senses [61, 54, 162]. Psychological distance has four dimensions: (1) temporal, (2) spatial, (3) social, and (4) hypothetical [12, 162]. The abstractness of these construals depends on their psychological distance from the self, namely the subjective perception that something "*takes place further into the future, [...] occurs in a more remote location, [...] happens to people less and less like oneself, and [...] is less likely to occur*" [163, p. 84]. Temporal distance refers to the perception that an event occurs at a time near (proximal) vs. far (distal) from the individual (e.g., the near vs. distant past or future). The greater the temporal distance, the higher the construal level used mentally to represent the object or event.

Duhigg [49] advises people to understand their habit loop if they want to break a habit. In particular, they should figure out what the cue is, and what reward the person gains from engaging in the habit, which confirms the influential factors mentioned by V5. For password creation as habit, the cue is clear: a screen asking them to formulate a new password to open an account for some service they want to use. The obvious reward is that they can satisfy their goals as quickly and easily as possible. The less obvious reward is that the password creation habit, if it exists, creates passwords with a measure of automaticity that is attractive to human cognitive misers [175], confirming V4. Habitual password creation routines are thus understandably resistant to change.

3.2 Change Readiness (Process Theory)

Norcross *et al.* [123] explain that individuals inhabit particular *stages of change*: (1) precontemplation, (2) contemplation, (3) preparation, (4) action and (5) maintenance. The person's current stage will determine how he or she reacts to a suggestion that a change be made in their existing routine. This kind of staged change readiness is also proposed by [29, 85, 102, 134].

If someone approaches a pre-contemplative person, assuming that he or she is in the contemplation or preparation stages, they are likely to drive individuals in the opposite direction and advice will be rejected [19, 58].

Norcross *et al.* [123] urge anyone wanting individuals to change behavior first to assess the person's readiness for change, because the most effective persuasive techniques to be used are different for people, depending on their current readiness stage. Yet it is understandable that

security awareness training is not delivered in this way due to the urgency of the issue and the fears around hackers compromising organizational systems. It might seem as if such an approach would be indulgent where such tolerance is simply too risky.

Many people do not understand why people with full knowledge of good practice will not unhesitatingly and willingly adopt it [110]. Their assumption is that "knowledge" as *cause*, leads to strong passwords, as *effect*. Yet the reality demonstrates that this particular cause (knowledge) is not sufficient to lead to the desired effect [11, 105] because the situation is far more complex than a mere lack of knowledge [22]. The same goes for assuming that the existence of a security policy will automatically lead to the desired effect: secure behaviors [181]. Both of these are necessary, but not sufficient, factors.

This confirms P1 and P3. Many organizations will retrain employees when they realise that initial training did not deliver the desired results, and find that more knowledge still does not invariably lead to stronger passwords across the board, demonstrating P2. Tsohou *et al.* [165], for example, find that cognitive and cultural biases shape risk perceptions and security behaviors, confirming the importance of understanding all the factors contributing to the process (P4, P5 and P6).

Change readiness exhibits the characteristics of process theory because people inhabit particular stages, and no amount of training, while necessary and essential, will make any difference to actual behaviors if the person is in a pre-contemplative stage. The transition from one stage to another can happen based on random events or interactions; stages and transitions are part and parcel of the essential process. For example, someone could be completely closed to any idea of change (Pre-Contemplative), but then have a random conversation with a close family member and subsequently be willing to contemplate listening to persuasive arguments (Contemplative) confirming P6. This would explain why, when educational drives often fail to make a difference, and the organization decides that more drives are necessary, these also fail to achieve their aim. More of a particular variable makes no difference when the situation is best described by a process theory (P2).

3.3 The Endowment Effect

There is a great deal of evidence to show that people place a higher value on artifacts they own than on those they do not own [2, 34, 59, 86, 101]. This phenomenon, termed "the endowment effect" is evidenced first by a reluctance to exchange owned artifacts for replacements [117]. The second consequence is evidenced by the difference between the amount of money people are

willing to accept (WTA) and how much they are *willing to pay* (WTP) for the owned (endowed) artifact, with the former exceeding the latter [2, 117].

This effect is not only triggered by endowed physical artifacts, but also by endowed time and routines [75, 118, 137], which makes it of interest in the password creation context. There is also evidence of the endowment effect being triggered by people self associating themselves with a brand [133]. Even when people were simply asked to associate themselves with a geometric shape did they subsequently associate different rewards with those shapes. It seems worth determining whether people associate their password routines with themselves, given the fact that this self association has proved so powerful in other contexts. If this is the case, it could well trigger an endowment effect as a consequence (P4, P6).

The endowment effect exhibits characteristics of process theory. We know it is triggered when someone feels that they own an artifact (required condition), but it does not infallibly do so (necessary, but not sufficient, to lead to the desired outcome) (P1). Arlen and Tontrup [10] suggest that the endowment effect only triggers when the person owning the endowed artifact has full responsibility for trading it for another. This seems to be another necessary, but not sufficient, condition. This demonstrates the importance of multiple factors preceding a desired outcome effect (P3). In the password field, ensuring that people know how to create strong passwords is also necessary, but not sufficient [66, 69, 70, 88, 114]. Knowledge thus constitutes a third necessary condition that needs to exist, yet there is no evidence that more knowledge invariably leads to more secure behaviors (P2; ¬V1).

Two of the pre-existing causes (ownership & responsibility) are either valid or not; there is no way of *varying or amplifying* these conditions. This kind of condition aligns with the tenets of process theory. In the case of the third condition (knowledge), it is clear that having more knowledge does not automatically map to improved password creation routines [74]. This breaks V3 of the variance theory, as enumerated in Table 1. Strahilevitz and Loewenstein [155] explain that the endowment effect increases with the length of time that the endowed artifact has been owned, which also suggests a longitudinal process rather than a single cause with a consequent deterministic effect, confirming P5.

Sometimes people do not feel endowed with an artifact, and so do not over-value it: the endowment effect is not triggered (P1). The variance theory would suggest that ownership will always lead to a feeling of endowment: that the outcome should be both predictable and certain (¬V6). If the endowment effect were explained by variance theory, ownership would be sufficient to trigger the endowment effect (¬V1). This does not occur, which suggests that variance theory does not apply when one considers the endowment effect outcome (¬V1).

Explanations for the endowment effect include:

- a feeling of *ownership* [112, 118]. Such a feeling could lead to a consequent sense of loss aversion [90] at the idea of losing the artifact, or an aversion to the regret that would be felt if a switch were made [155]. Some have suggested that the sunk cost effect comes into play, preventing people from making a change [9, 187].

- individuals feeling a psychological *attachment* to what they own [145, 152] especially if they have owned the artifact for any significant period of time [95, 155]. Chatterjee *et al.* [35] suggest that attachment and ownership interact to evidence as the endowment effect.

- the idea that ownership somehow bolsters *self image* [6, 35, 132], or that people associate the owned artifact with themselves [18, 108]. They might well use it to signal competence [116].

  The observable effect of such over-valuing is that the owner will react to a switching suggestion by focusing on the positive aspects of the owned artifact [23, 50, 81, 121, 125], while, at the same time, highlighting the potential negative outcomes of switching [189]. In general, this manifests as change resistance [93] and an apparent discounting of advice [21, 147, 186, 185] when a suggestion of a switch or a swap is made. Consider how this would apply to password creation. Jan comes up with an algorithm to create passwords, and having done so, and liking the positive aspects of using this mechanism, decides to adopt it: a self-endowment as it were. Brehm [26] explains that, having made a choice, Jan is likely to emphasize the positive aspects of the chosen routine, and the negative aspects of the discarded routines. When someone comes along and tries to convince Jan to adopt another password creation mechanism Jan still focuses on the most negative aspect of the new mechanism [23], which might well include the cost, in terms of time and effort, of adopting the new routine.

Consequences of the endowment effect (endowment calculus outcomes) include:

1. the *utility of the artifact being over-estimated*, particularly by subjective *perceptions of risk* [91].

   Prior experimental research has investigated the interplay between risk, loss aversion, and endowment effects, but much of that research treats risk and endowment as orthogonal independent variables (e.g., [97, 149]). Moreover, much of that risk-related economic and psychological research employs experimental designs in which subjects participate in

lotteries with known objective probabilities (e.g., outcomes are dependent on dice rolls [7]).

Past endowment research strongly suggests that feelings of endowment are produced "*apparently instantaneously*" [166, p.1041],[89, 128] while risk judgments are "*constructed ... through a combination of affective and analytic evaluations of risky options*" [57, p.142]. As the product of an extended cognitive process, perceived risk is thus more akin to change willingness than it is to endowment. Accordingly, perceived risk will be conceptualized in our study as an outcome of an endowment calculus.

2. reluctance to adopt new routines (i.e. *change unwillingness*, which is the main outcome of the endowment effect), as revealed in other studies where people decline to make a change because they have already made a choice and want to stick with it [26, 117, 148]. Kahneman *et al.* [90] refer to the endowment effect as the *status quo* bias.

3. the owned artifact will be *over-valued*. For physical artifacts, this is evidenced by the difference between WTA and WTP. For time, it is evidenced by people wanting more payment for their own time spent than they think others should be paid for the same labor taking the same amount of time [75].

3.4 Risk

People tend to engage in behaviors based on their perceptions of the risks related to the behavior [142, 183]. Risk perceptions thus play a vital role in predicting whether or not people will engage in precautionary behaviors [24]. A password is intended to prevent people from accessing a resource or service using someone else's identifier. As such, it is essentially a risk management mechanism. Van Schaik *et al.* [170] identified a number of predictors of precautionary cyber security behaviors. Other researchers have carried out similar studies, also identifying particular predictors [67, 79, 164, 103]. These studies confirm a link between risk perception and precautionary behaviors.

Yet other studies have failed to find evidence for this relationship [40, 72, 33]. Hence we considered it appropriate to include a tool to measure risk perception in our model, and to determine the interdependencies between risk perception and the other constructs we are measuring.

3.5 In Summary

We have reviewed three potential explanations for a reluctance to adopt new security routines. Each is likely to play a role, as do others. All deserve research attention and full investigation. We chose to focus on the endowment effect and the role it potentially plays in triggering change resistance related to password creation routines.

To determine whether the endowment effect is indeed triggered by the password creation request acting as a cue, we will gather evidence by extrapolating from measures used to test endowment of physical artifacts that people own, as well as measures to assess risk perception.

4 Investigating the Endowment Effect

We sought evidence for the triggering of the endowment effect in the following phenomena:

1. H1: people have *pre-existing routines* for creating passwords.
2. H2: people are "endowed" with their routines i.e.
   (a) they feel a sense of *ownership* with respect to their pre-existing routines.
   (b) they feel *attached* to their routines.
   (c) they *over-value* their routines.
   (d) their routines are connected to their personal *self image*.
3. H3: people will exhibit *endowment calculus* outcomes based on the extent to which they are "endowed" with their routines i.e.
   (a) they will exhibit *decreased perceived risk*.
   (b) they will be *less willing to switch routines*.

To find evidential support for these hypotheses, we designed several survey instruments, whose questions are shown in the Appendix. Figure 2 details all the tested hypotheses.
We conducted three surveys:

1. **Survey 1 — Determine that Pre-Existing Routines Exist & Explore Routine Types**: Qualtrics Survey with 106 student respondents. We embedded attention questions to weed out unthinking responses. This left 98 responses for analysis (32% Male, 68% Female).

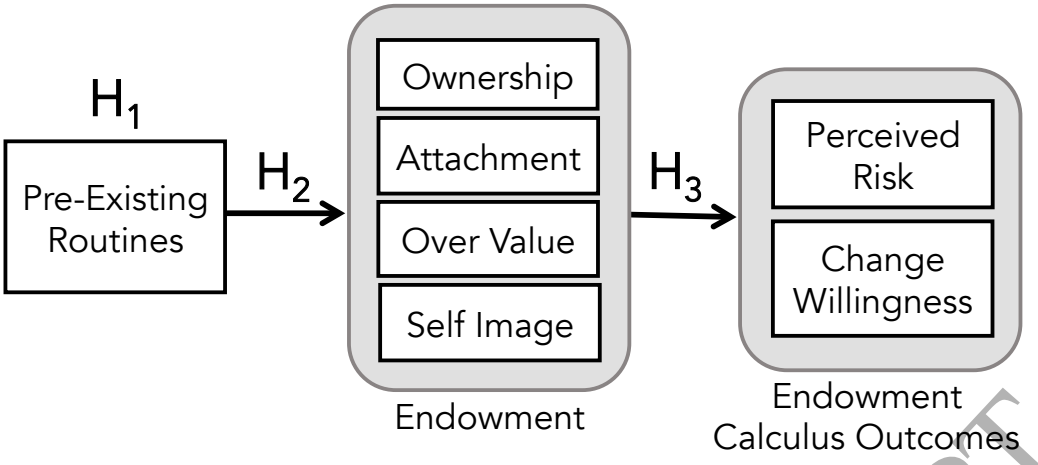

Figure 2: Model 1 (Hypotheses to be Tested).

2. **Survey 2 — Confirm Routine Existence & Explore Reasons for Resistance**: Mechanical Turk survey. We received 313 responses. After removing those that failed attention questions or suggested nonsense responses, we were left with 300 responses (63% Male, 37% Female).

3. **Survey 3 — Test for Endowment Calculus Outcomes**: Mechanical Turk survey. We received 332 responses. After removing records where people had failed attention questions, we were left with 301 responses to support analysis (60% Male, 40% Female).

Measurement Constructs

The questions posed to assess the core constructs are provided in the Appendix. For all questions, the order of options was randomized. Attention questions were embedded to weed out unheeding responses. We also filtered out responses that were extreme outliers when the survey was completed within seconds rather than the 5-10 minutes it ought to have taken.

Ownership: Questions (O1, O2, O3) were adapted from those proposed by Van Dyne and Pierce [168].

Attachment: Thomson *et al.* [159] explain that a sense of attachment manifests in expressions of an emotional reactions towards the artifact. For example, attachment leads people to want to preserve their relationship with the artifact and to feel favorable and loyal towards it. They are also likely to be satisfied with the artifact, and express a sense of involvement with it. We thus tested this construct with questions: A1 (favorability), A2 (continuance of relationship), A3 (loyalty) and A4 (satisfaction).

Perceived risk: The questions (P1, P2, P3) were adapted from those used by Johnston and Warkentin [87].

Change willingness: There are measurement constructs for "openness to change" [80], but they will not measure willingness to change password routines, in particular. Hence we asked about *willingness* to change (C1 — openness), *plans* to change (C2 — definite future) and *predictions* of change (C3 — probable future).

4.1 H1: Pre-Existing Routines

We first posed a question to determine whether people had their own pre-existing routines for password creation:

Survey 1 Question: Do you have a usual practice for CREATING your passwords? 66% said yes, 25% said no, and 8% were unsure.

We then elicited more information about their routines. First, we asked them how similar their password creation routines were to a number of strategies, rating them as (1) Nothing like mine, (2) Minor Similarities, (3) Some Similarities, (4) Similar and (5) Identical. The numbers of participants who chose these are shown in Figure 3. Interestingly, of the 25 people who claimed not to have a routine in Survey 1, 12 picked one of the strategies mentioned in Figure 3, which suggests that they actually *did* have a routine.

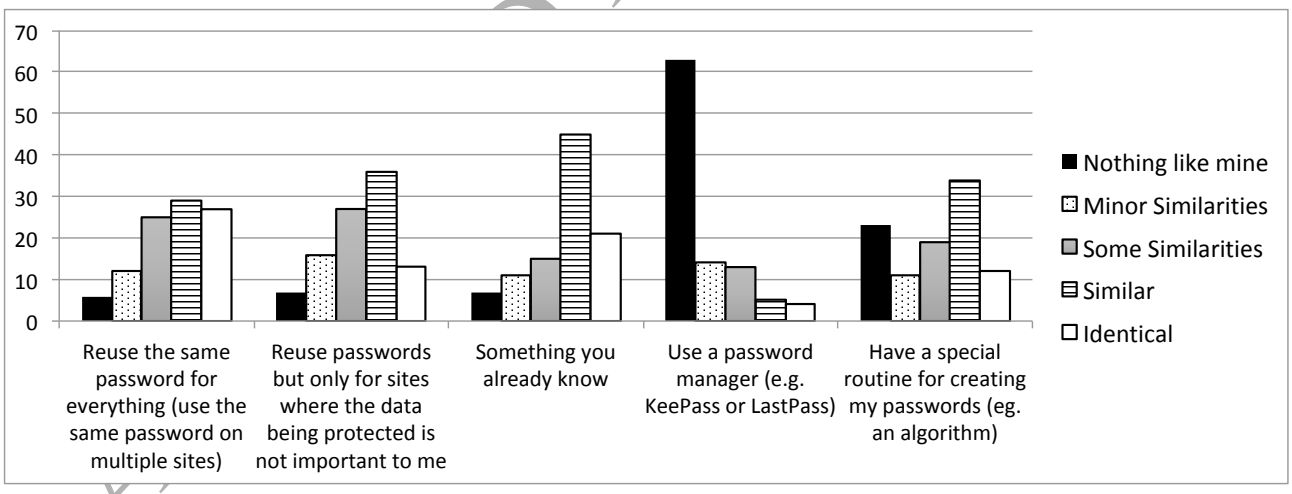

Figure 3: Password Creation Routine Types.

If they indicated similarity to "what you know", we followed up by asking them whether their strategy was similar to a number of options, as shown in Figure 4. If they indicated an algorithm, we followed up by offering them the options shown in Figure 5. (People could choose multiple strategies).

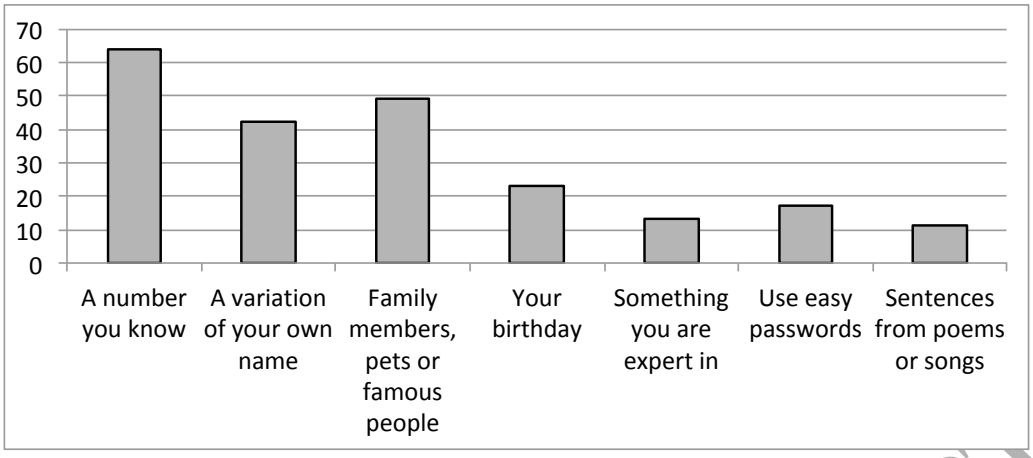

Figure 4: "What You Know" Password Creation Routines.

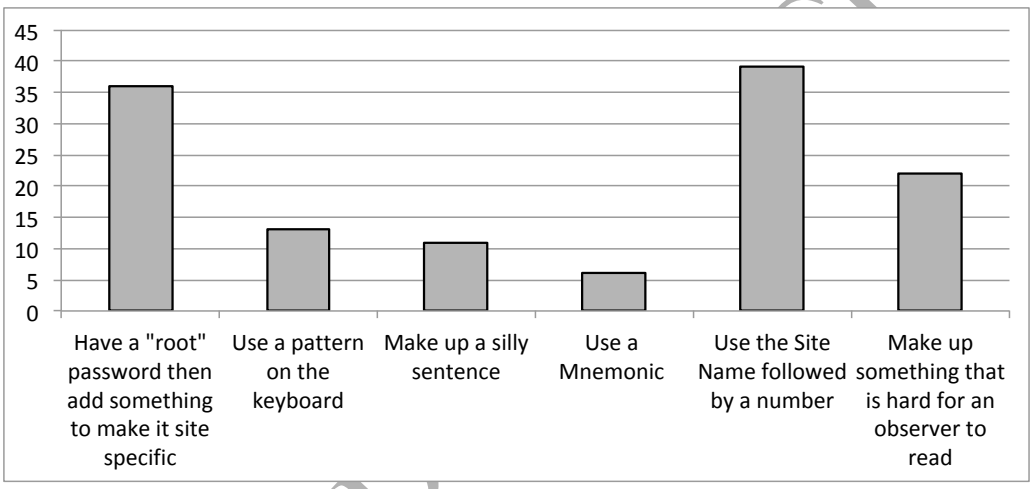

Figure 5: Algorithmic Password Creation Routines.

Survey 2 Question: (Confirming Survey 1's finding) Do you have a usual practice for CREATING your passwords? 84% said yes, 14% said no, and 2% were unsure. This confirmed that a majority of our respondents did indeed claim to have their own usual routine for creating passwords.

Evidence from our two surveys, augmented by multitudinous online comments, suggests that H1 can be accepted.

4.2 H2: Endowment Effect

Ownership & Attachment

The questions posed in Survey 3 to assess ownership and attachment are shown in the Appendix. Figure 6 depicts responses to the "ownership" questions, and Figure 7 depicts responses to the

"attachment" questions. In both cases responses suggest that not only do most respondents possess routines (confirming H1), but that they feel a sense of ownership of, and attachment to, such routines.

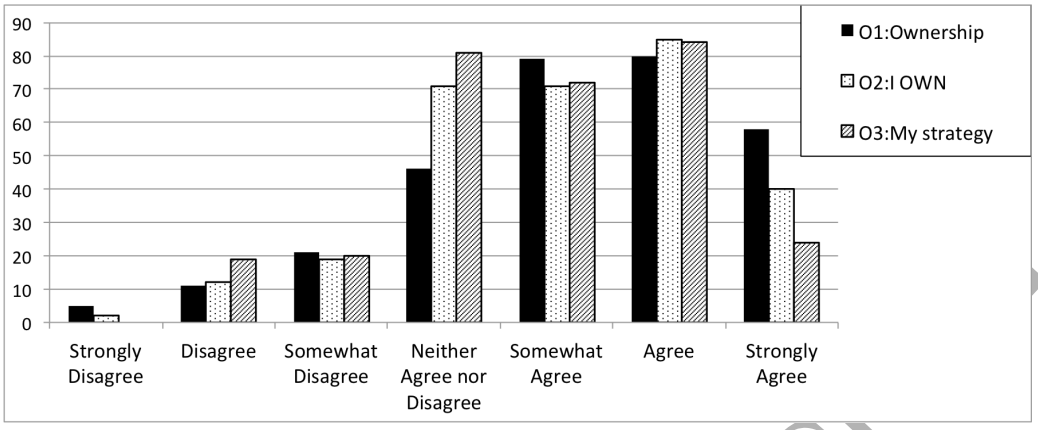

Figure 6: Agreement with Ownership Questions.

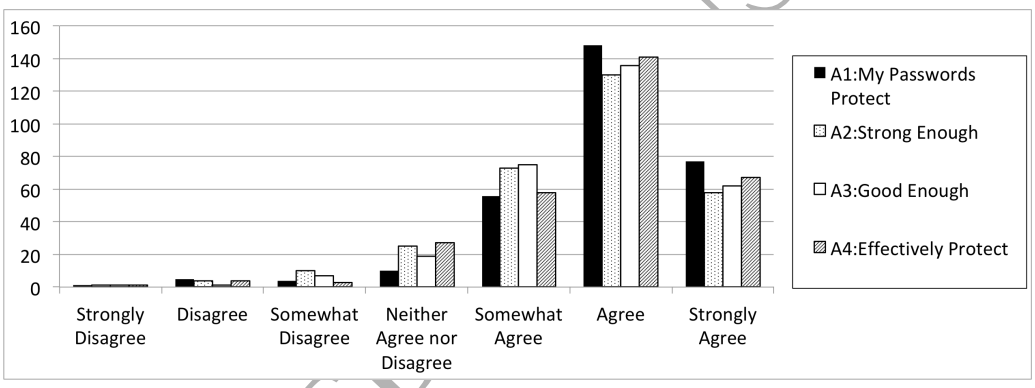

Figure 7: Agreement with Attachment Questions.

Over-Valuing

We tested this aspect in Survey 3 by approximating the usual (WTA-WTP) payment scenarios used to test the endowment effect for physical artifacts. It would have been ideal if we could have used one of the pre-existing WTA:WTP comparisons that other endowment studies use, but the snag is that one does not relinquish a routine as one relinquishes a physical object if one decides to trade it, so there was no direct mapping for us to use.

Hence we set up a scenario where we "paid" people for the effort it would take to switch. we were testing whether respondents considered *their* time and effort more valuable than that of other people. In this case, therefore, the effort that went into developing the existing password creation routine is the endowment.

As stated earlier, the difference between routine endowment and physical object endowment is that, with a physical artifact, the person sets the WTA price based on the assumption that if he/she sells the artifact, he/she will no longer own it or have access to it. Of course with routines this is unrealistic: changing a routine does not mean relinquishing access to the previous routine.

We had to come up with an approximation, as follows. We would determine how much money people would be willing to accept to change their routine. In this case, they are not paid to give up their routine for good; they are being paid for being willing to learn a new routine, and to adopt it in the future. This is not a perfect compromise, but, comparing what other people should be willing to accept to do this, and what the person him/herself should be willing to be paid, we can detect a difference.

We used this approximation hoping that it would give us some indication of whether the person was *endowed* with their pre-existing routine.

We first set the scene by asking them to imagine that a bank had decided to pay people to choose stronger passwords. We then asked them to fix on an amount *they* were willing to accept and an amount the bank would have to pay *other people* to be willing to do this. The full question is provided in the Appendix. Table 2 details the descriptive statistics of their responses to the two questions.

Tests for normality (Shapiro-Wilk) showed that neither set of values was normally distributed ($p<0.001$). We used a Wilcoxon signed rank test to carry out pair-wise comparisons. This showed that WTA was significantly greater than WTP for changing their password creation routine ($p=0.007$). Thus, using the same mechanism as that used to test endowment for physical artifacts, we showed an endowment effect was likely to be triggered for pre-existing password creation routines.

	N	Min	Max	Mean	StdDev
Pay Others	290	0	500	23.05	43.52
Pay Me	290	0	1500	28.78	104.013

Table 2: Descriptive Statistics for 'Pay Others' vs. 'Pay Me.'

Self-Image

Here, we used a scenario-based question. Alexander and Becker [5] argue that scenario questions are useful when researchers are attempting to approximate real-life decision-making situations,

especially when the decision being measured might have social desirability undertones [78]. Trevino [160] makes the point that it is sometimes better to use a scenario than a direct question in these cases. The scenario method allows us to pose questions indirectly, to trigger realistic responses. Scenario questions have been used in other information security studies [14, 15, 44, 55, 87, 98, 161, 180].

We created a scenario with two people arguing about how they create their passwords[1], as follows: "*Terry and Pat are talking about how they create their passwords. Terry's and Pat's ways of coming up with new passwords are very different. Terry says to Pat: 'Your way is just plain wrong!'*" We then offered respondents eight options, and they could select as many as they liked (randomly ordered except for the final one):

a) Pat retorts "My way is better than yours."

b) Pat says "My way is good enough."

c) Pat feels hurt.

d) Pat changes the subject.

e) Pat ends the conversation and walks away.

f) Pat says "Explain why it is wrong."

g) Pat says "Tell me more so I can adopt your way."

h) None of the above, please explain.

The first five options suggest self protection responses [150] in line with Pat becoming defensive (a,b), avoiding (c,d) or withdrawing (e). These are all signs of 'Pat' feeling that his/her self image is connected in some way with a particular behavior. We were hoping to elicit the respondent's personal feelings that their own self is threatened by the exchange with 'Terry', and responding in a way that would reduce the threat. The sixth response suggests a willingness to listen to why their routine is wrong, and the seventh reflects a willingness to adopt a different routine. The final option allows them to nominate their own response.

Five people chose the "None of the Above" option but did not provide an explanation. Figure 8 shows the number of people who selected at least one self-defense option, those who selected option (f) (Listening) or option (g) (Adopting).

[1]These names have been chosen specifically to ensure gender equality

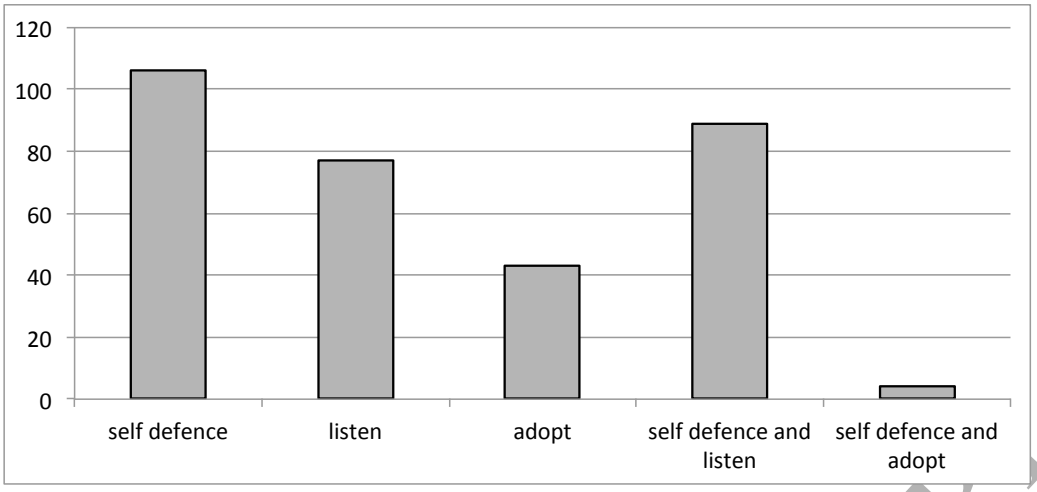

Figure 8: Responses to having Password Creation Routine Challenged.

The most common response is a self-defense option: avoiding, feeling hurt, feeling defensive or withdrawing. The second most chosen combination is self-defense followed by a request for Terry to explain the assertion. 15% chose the adoption response. What is particularly interesting is that a very small number (4) checked both self-defense and adoption options. This suggests that if an attack on a person's routine invokes a self-defense response, subsequent adoption is unlikely as a next step.

4.3 H3: Change Resistance

Surveys 1 & 2

We posed a question in both Surveys 1 and 2 to get a feel for the level of change resistance ("I *don't* want to change the way I create passwords?"). The average of all responses in Survey 1 was 5.2 (between "Somewhat Agree" and "Agree"). The median and mode were both 6 (Agree). The average over all responses in Survey 2 was 4.98, with a mode of 6 (Agree) and a median of 5 (Somewhat Agree). This suggests a general but not strong *unwillingness* to consider changing their password creation routine. The percentages of different responses are shown in Figure 9. The profile is somewhat different for the two cohorts, perhaps due to their different make-up: Survey 1 respondents were students, Survey 2 respondents were Mechanical Turk workers.

We asked people why they would be unwilling to switch routines (proffered options presented in random order). Their responses are depicted in Figure 10. It is interesting that the most popular option was one that referred to the person's pre-existing routine. The second most

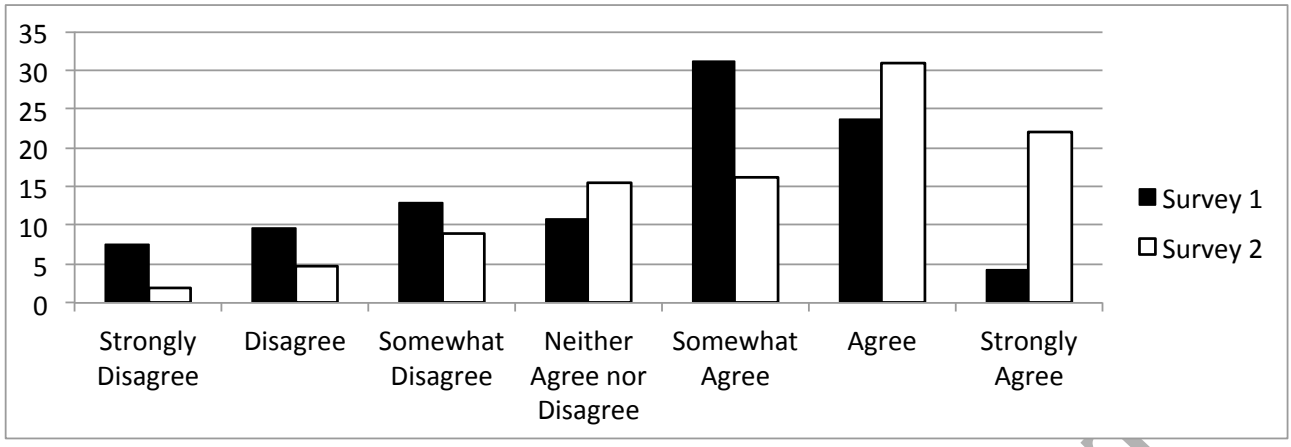

Figure 9: Please indicate your agreement with the following statement: I don't want to change the way I CREATE passwords (Shown as Percentages).

popular option suggests that people are content with their own routine. Two people chose the "Other" option, offering the following comments: '*Every outfit seems to have different requirements and keeping track of them all is a hassle*', and '*More difficult to retain*'

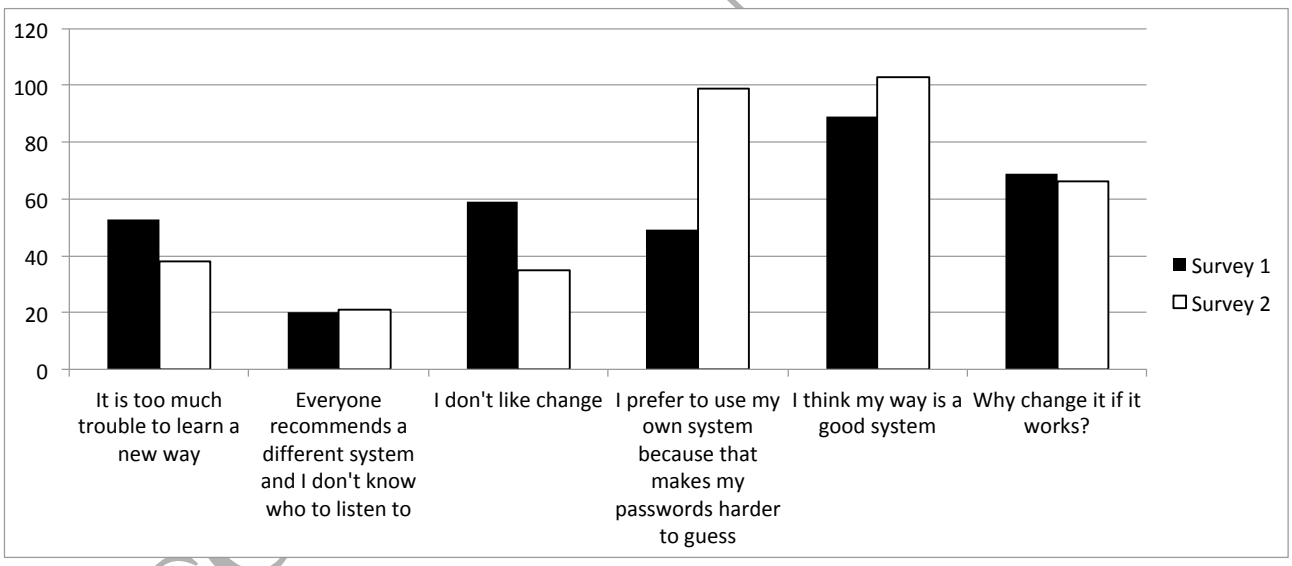

Figure 10: Reasons for Unwillingness to Change.

Survey 3: Perceived Risk and Unwillingness to Change as Endowment Effect Outcomes

We examined the effects of Attachment and Ownership on Perceived Risk and Change Willingness the better to understand the role of endowment effects on those outcomes. The effects of Self-image and Over Value were not examined because their measurement items were not

normally distributed and thus not amenable to maximum likelihood estimation in structural equation models [32].

Given the newness of our Attachment and Ownership constructs, an exploratory factor analysis (EFA) with Varimax rotation comparing those factors against Perceived Risk and Change Willingness was performed using IBM SPSS v. 24.0.0.0. Results from the EFA and reliability tests assessing Coefficient α both support the convergent and discriminant validity of those four variables (Table 3).

	Coeff α^a	CR[b]	AVE[c]	Attachment[d]	Ownership	Perc'd Risk	Change Willingness
Attachment	0.84	0.83	0.46	0.68			
Ownership	0.88	0.89	0.72	0.51	0.85		
Perc'd Risk	0.72	0.71	0.45	-0.37	-0.03	0.67	
Change Willingness	0.80	0.81	0.59	-0.09	0.13	0.56	0.77

[a] Coefficient alpha

[b] Composite Reliability

[c] Average Variance Extracted

[d] Diagonal elements in Columns 5-8 are the square root of the AVE. Non-diagonal elements are factor correlations

Table 3: Descriptive Statistics for Survey 3's Measurement Model.

Additional convergent and discriminant validity tests were conducted using a measurement model for the Attachment, Ownership, Perceived Risk, and Change Willingness variables. This model was tested using IBM SPSS Amos v. 24.0.0. Modification indices indicated high correlations between three sets of error terms for the Attachment construct. These were allowed to correlate in subsequent measurement and structural models.

Results from the second measurement model analysis were used to assess Composite Reliability (CR), Average Variance Extracted (AVE), and factor correlations. These statistics were calculated using Gaskin's Excel-based Stats Tools Package [68]. In the initial analysis, the AVEs for Attachment and Perceived Risk were slightly below the desired threshold of 0.50. However, the CRs for those two variables were above 0.70, indicating that convergent validity was adequate for our exploratory study. The correlations between the four latent variables were

all below the square root of the corresponding AVEs, thus supporting discriminant validity.

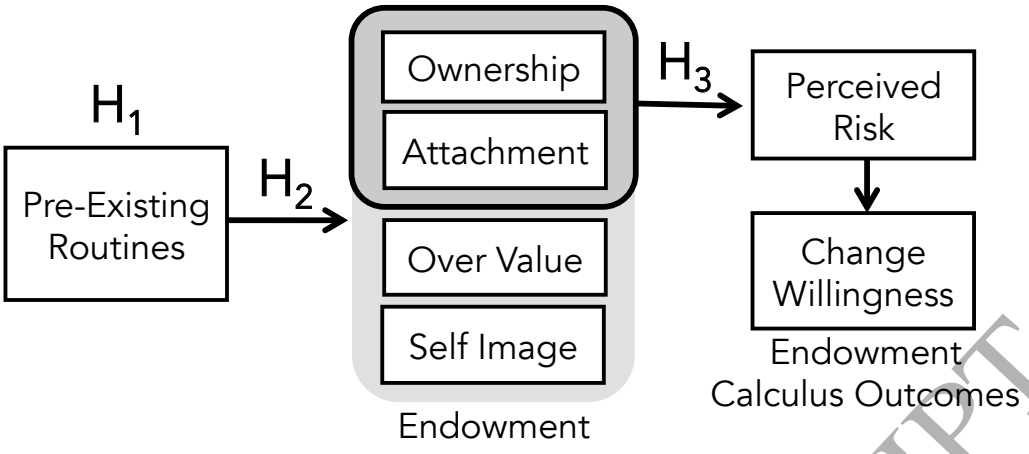

Figure 11: Model 2 (Post-Hoc Structural Model).

χ^2	*df*	*p*	GFI	CFI	TLI	RMSEA
Model 1 (Original Structural Model)						
240.58	81	0.000	0.90	0.92	0.89	0.08
Model 2 (Post-Hoc Structural Model)[a]						
188.94	80	0.000	0.92	0.94	0.93	0.07

[a] χ^2 Model 1 - χ^2 Model 2 = 240.5881 – 188.9480 = 51.641, p < 0.001

GFI: Goodness Fit Index

CFI: Comparative Fit Index

TLI: Tucker Lewis index

RMSEA: Root Mean Square Error of Approximation

Table 4: Goodness of Fit Statistics for Survey 3's Structural Model.

Hypothesis 3 was tested using a structural model based on Figure 1 and Table 2. Modification indices indicated the original structural model (Model 1 — Figure 2) could be significantly improved by adding a path between "Perceived Risk" and "Change Willingness" (Model 2 — Figure 11). Though not part of the original H3, the addition of this path is supported by research indicating that endowment effects are associated with perceived risks (e.g., [173]) and that risk can be a predictor of change readiness (e.g., [136]). Given the exploratory nature of our study, we deemed it appropriate to test this improved Model 2. Goodness of fit values for

Models 1 and 2 are displayed in Table 4. Goodness of Fit statistics for the improved model suggests it exhibits adequate fit for our exploratory research. The difference in χ^2 between the original and post-hoc structural models indicates significant improvement of Model 2 over Model 1 ($p < 0.001$).

Standardized regression and explained variance statistics (i.e., B and R2, respectively) from Models 1 and 2 are compared in Table 5. Perhaps the most striking finding is that the B values for "Attachment → Change Willingness" and "Ownership → Change Willingness" both change from significant at the $p < 0.001$ level in Model 1 to non-significant in the post-hoc Model 2. The B values for the Attachment → Perceived Risk and Ownership → Perceived Risk remain largely unchanged. Taken together, these findings indicate that Perceived Risk fully mediates the relationships between Attachment → Change Willingness and Ownership → Change Willingness. Coupled with these mediation effects is the observation that the R^2 of Change Willingness in Model 2 is not only meaningful, but that it is more than three times larger than that of Model 1.

	Dependent Variable			
	Perceived Risk		Change Willingness	
Predictor Variable[a]	Original Model	Post-Hoc Model	Original Model	Post-Hoc Model
Attachment	-.054 (<0.001)	-0.52 (<0.001)	-0.31 (<0.001)	0.09 (0.589)
Ownership	0.28 (<0.001)	0.25 (<0.001)	0.30 (<0.001)	0.09 (0.273)
Perceived Risk	N/A	N/A	N/A	0.58 (<0.001)
Variance Explained Statistics				
R^2	0.21	0.20	0.09	0.32

[a] Standardized regression weights. p-values are displayed in parentheses.

Table 5: Path Statistics for Survey 3 Structural Model.

As expected, Attachment is negatively associated with Perceived Risk in Model 2 (i.e., Attachment is associated with a more positive valuation of their existing password creation routine). Ownership, on the other hand, is positively associated with Perceived Risk. This

surprising contradiction confirms the complexity of the endowment effect, a finding that is reported in other research [57, 90].

5 Discussion, Reflection & Future Work

Pre-Existing Routines: Our research question explored whether individual computer users had their own pre-existing routines for creating their authentication passwords, and the responses certainly showed that the majority of our respondents did feel that they had such routines (Section 4.1). Though not a universal finding, two of our surveys confirmed this assertion.

Evidence for endowment effect: Having confirmed the existence of routines that people considered to be their usual practice, we then set out to find evidence of their own endowment effect, in terms of endowment calculus outcomes. Responses to ownership and attachment questions demonstrated agreement with these sentiments. We also showed that they tended to over-value their existing routines. This was confirmed by their stated unwillingness to change routines, reported in Section 4.3. We also showed that their WTA was significantly greater than WTP, when it came to the effort involved in changing password creation routines (Section 4.2).

Confirmation of Artifact-Based Causatives: In Figure 10, we see some of the same explanations for routine endowment as we saw in the literature related to endowed physical artifacts. Most respondents valued their own password creation systems, and focused on the negative aspects of switching to a new routine. They referred to their own system working well enough ("*why change? prefer to use my own*"), and the negative consequences of changing ("*too much trouble*"). They also mentioned the uncertainty related to switching ("*don't know who to listen to*"), one of the causes of the endowment effect mentioned in Section 3.3.

Our earlier exploration of the theoretical background for understanding the role of the endowment effect in inhibiting the adoption of newer, and perhaps better, routines for creating authentication passwords highlighted the complexity of this phenomenon, the psychological nuances of the conscious and nonconscious decision processes that individuals pursue, and the difficulties in isolating the relationships between the various contributing factors that have prevented researchers from finding clarity and certainty in studies of endowment, including our focal context of password creation routines. The human mind is indeed mysterious. Nevertheless, our findings have shed some light on this complex nomological conglomeration. The insights that surfaced from our investigation reinforce that there are both variance (associa-

tion) explanations and process (stage) explanations for why users want to retain their current password creation routines. Our results show the covariance relationship between ownership and attachment (variance), for example, and we also suggest a mediation role for perceived risk in the thought process of individual users making this decision (process). Further, we noted earlier that perceived risk was conceptualized as an outcome of an endowment calculus, and we measured it by asking respondents to consider their password creation routines in contrast to "other routines" in terms of robustness against hackers, with results that confirm our hypothesis. This certainly implies that users assessed alternatives subsequent to the establishment of their current routines when considering alternatives (a process), which may occur repeatedly when confronted with novel information about password creation alternatives.

Reflection: In numerous other voluntary (not mandatory) technology adoption or change decisions, individuals make the decision to switch. For example, evidence shows that millions of users switched their primary web browser [28] (Internet Explorer was once dominant, and now has a small market share). It is possible that password creation possesses certain salient characteristics unlike other change decisions. For one thing, users' perceived psychological ownership may convey a sense of personal identity manifestation (self image) on a password creation routine that individuals feel they have designed for themselves [108]. Internet Explorer, on the other hand, was installed by default on Windows machines, and its initial widespread use could be explained by the fact that most people stick with the default option [46].

Individuals may almost take some sense of personal pride in their personal development of a password creation routine [124]. For another thing, switching costs may be very high, especially as we all experience a proliferation of accounts and memberships requiring password authentication. This, again, not being similar to the relatively painless switching of other kinds, such as preferred browser.

The post-hoc finding that perceived risk fully mediates the relationships between endowment effects and change willingness needs further exploration. Several research domains may be instructive in this regard. For example, investigations examining the role of affect in endowment effects (e.g., [57, 92]) may be especially fruitful. Research on the privacy calculus model (e.g., [42, 47]) may provide a rich context for future exploration of endowment effects, perceived risk, and change willingness.

When we used a scenario to elicit responses to someone scotching a pre-existing routine (testing the fact that the routine is linked to self image), we saw that people experienced it as a threat, which was demonstrated by the majority choosing a self-protection response (Section 4.2). We also showed that such a response was unlikely to lead to adoption, based on the

choices made by the respondents.

Theories: We commenced this paper by considering two types of theories that could explain reluctance to adopt new security behaviors: variance and process (Section 3). We discussed how the endowment theory had much in common with process theory since it required knowledge, ownership and responsibility for trading to precede triggering of the effect. Given the outcome of our investigation, we can confirm that, in the case of password creation routines, the situation is best described by process theory. Many of our respondents demonstrated that they felt they owned their personal routines, and felt attached to them. Moreover, there was evidence that they over-valued the routines and self-identified with them (P1). The endowment effect was thus triggered, demonstrating that these causes preceded the effect, but with no certainty since a minority of our respondents did not feel endowed with their personal password creation routines. This means that the effect was not certain, as one would expect it to be if it were described by variance theory (¬V1, ¬V3, P3).

Future Work: The relationship between password creation routines and password storage and recall routines warrants further scientific investigation. Creating a password is fundamentally tied to the recall of that password, as users seek to create passwords they can remember. If users were offered a new creation method that created passwords which were intrinsically easier to remember, the decision calculus may conceivably tilt in favor of switching.

Another avenue for future work is the exploration of the role of the endowment effect as it relates to other security behaviors. Do users have a sense of ownership over the method they use to back up their data? What would it take to convince a user to start using an alternative method to secure their data in these and other ways? We could also consider how they patch their software, or how they determine if an email is legitimate or a phishing attempt.

This investigation offers some interesting insights which make the endowment effect worth pursuing further, especially in this context. We intend to carry out further investigations into the potential impact of the endowment effect, both in terms of password creation and also other security routines. Finally we want to pursue mitigation measures that could be used to minimize or neutralize its impact.

6 Limitations

We used a combination of existing and new scales and items to measure the endowment effect of artifacts in our study. These scales may not be robust and highly refined when adapted to this unique context. Further scale development and testing is could sample a more diverse audience

(e.g., across organizational units and hierarchical levels) than our use of students and the Mechanical Turk system. Additional techniques – particularly qualitative studies – could elicit additional perspectives regarding endowment in ways that can increase scale generalizability and deepen our understanding of endowment effects.

Similar recommendations apply to our assessments of perceived risk. Our tests of perceived risk, as a predictor of change willingness, is predicated on modification indices from a *post-hoc* analysis of our structural equation modeling results. Those associations were subsequently confirmed by findings in the literature. For example, associations between endowment/ownership effects on risk perceptions are described in [16, 90], while associations between risk perceptions and judgments/intentions are described in [90, 91]. Nonetheless, more theoretically rigorous tests should be conducted in the context of information security to confirm these findings. As with our above recommendations concerning endowment, additional scale development research using more diverse samples across organizational units and hierarchies could support a deeper understanding of risk perceptions in the context of information security and endowment effects.

Many organizations, websites, and apps that require passwords impose constraints and mandatory processes for password creation and use that may supersede our findings. Biometric authentication (and other emerging technologies) may make the use of passwords obsolete, or at least less important in the future. Nonetheless, a number of information security threat mitigation procedures may still be susceptible to endowment effects (e.g., ways to identify and avoid email phishing attacks or malicious Web sites). The extent to which endowment effects may compromise organizational efforts to resist such threats remains to be determined. Moreover, the cat-and-mouse nature of information security suggests that new challenges will arise over time, and that some of them may be susceptible to endowment effects.

7 Conclusion

This paper reports on an investigation into whether the endowment effect is a possible explanation for change resistance when it comes to password creation. We did indeed find evidence for pre-existing routines, change resistance, and an endowment effect calculus.

We thus conclude that initial evidence points towards the likelihood that people do indeed feel endowed with their password creation routines. We suggest that further experiments be carried out to confirm or deny our findings, and explore an endowment effect influence when it comes to other security routines.

In concluding, we reiterate that the endowment effect is merely one of a host of factors that

can contribute towards people's reluctance to adopt more secure password creation routines. Others, some of which are reviewed in Section 2, will undoubtedly also come into play. More research will need to be carried out to confirm their influence in the cyber security arena, and in understanding how they might interact with and reinforce or neutralize each other.

Acknowledgements & Ethics

This research was carried out while the first author was a Fulbright Scholar at Mississippi State University (MSU). The surveys were approved by the Institutional Review Board of the same University. We thank the academics at MSU, who reviewed our survey questions and helped us to improve and refine them.

References

[1] H. Aarts, B. Verplanken, and A. Knippenberg. Predicting behavior from actions in the past: Repeated decision making or a matter of habit? *Journal of Applied Social Psychology*, 28(15):1355–1374, 1998.

[2] W. L. Adamowicz, V. Bhardwaj, and B. Macnab. Experiments on the difference between willingness to pay and willingness to accept. *Land Economics*, 69(4):416–427, 1993.

[3] E. Albrechtsen. A qualitative study of users' view on information security. *Computers & Security*, 26(4):276–289, 2007.

[4] E. Albrechtsen and J. Hovden. The information security digital divide between information security managers and users. *Computers & Security*, 28(6):476–490, 2009.

[5] C. S. Alexander and H. J. Becker. The use of vignettes in survey research. *Public Opinion Quarterly*, 42(1):93–104, 1978.

[6] T. Alexopoulos, M. Šimleša, and M. Francis. Good self, bad self: Initial success and failure moderate the endowment effect. *Journal of Economic Psychology*, 50:32–40, 2015.

[7] V. Anderhub, W. Güth, U. Gneezy, and D. Sonsino. On the interaction of risk and time preferences: An experimental study. *German Economic Review*, 2(3):239–253, 2001.

[8] D. Ariely and M. I. Norton. How actions create – not just reveal – preferences. *Trends in Cognitive Sciences*, 12(1):13–16, 2008.

[9] H. R. Arkes and P. Ayton. The sunk cost and Concorde effects: Are humans less rational than lower animals? *Psychological Bulletin*, 125(5):591–600, 1999.

[10] J. Arlen and S. Tontrup. Does the endowment effect justify legal intervention? The debiasing effect of institutions. *The Journal of Legal Studies*, 44(1):143–182, 2015.

[11] M. Bada and A. Sasse. Cyber security awareness campaigns: Why do they fail to change behaviour?, 2014. Global Cyber Security Capacity Centre, University of Oxford, Retrieved 24 Dec 2018 from `http://discovery.ucl.ac.uk/1468954/`.

[12] Y. Bar-Anan, N. Liberman, and Y. Trope. The association between psychological distance and construal level: evidence from an implicit association test. *Journal of Experimental Psychology: General*, 135(4):609–622, 2006.

[13] J. A. Bargh, P. M. Gollwitzer, A. Lee-Chai, K. Barndollar, and R. Trötschel. The automated will: nonconscious activation and pursuit of behavioral goals. *Journal of Personality and Social Psychology*, 81(6):1014–1027, 2001.

[14] J. B. Barlow, M. Warkentin, D. Ormond, and A. R. Dennis. Don't make excuses! Discouraging neutralization to reduce IT policy violation. *Computers & Security*, 39(B):145–159, 2013.

[15] J. B. Barlow, M. Warkentin, D. Ormond, and A. R. Dennis. Don't even think about it! The effects of anti-neutralization, informational and normative communication on information security compliance. *Journal of the Association for Information Systems*, 19(8):308–327, 2018.

[16] M. H. Bazerman and J. J. Gillespie. Betting on the future: the virtues of contingent contracts. *Harvard Business Review*, 77(5):155–60, 1999.

[17] A. Beautement, M. A. Sasse, and M. Wonham. The compliance budget: managing security behaviour in organisations. In *Proceedings of the 2008 Workshop on New Security Paradigms*, pages 47–58. ACM, 2009.

[18] J. K. Beggan. On the social nature of nonsocial perception: The mere ownership effect. *Journal of Personality and Social Psychology*, 62(2):229–237, 1992.

[19] L. E. Beutler, T. M. Harwood, A. Michelson, X. Song, and J. Holman. Resistance/reactance level. *Journal of Clinical Psychology*, 67(2):133–142, 2011.

[20] G. Binder and J. M. Boldero. Planning for change: the roles of habitual practice and habitus in planning practice. *Urban Policy and Research*, 30(2):175–188, 2012.

[21] S. A. Birch and P. Bloom. The curse of knowledge in reasoning about false beliefs. *Psychological Science*, 18(5):382–386, 2007.

[22] J. Blythe, R. Koppel, and S. W. Smith. Circumvention of security: Good users do bad things. *IEEE Security & Privacy*, 11(5):80–83, 2013.

[23] P. Bordalo, N. Gennaioli, and A. Shleifer. Salience in experimental tests of the endowment effect. *The American Economic Review*, 102(3):47–52, 2012.

[24] S. Boss, D. Galletta, P. B. Lowry, G. D. Moody, and P. Polak. What do systems users have to fear? Using fear appeals to engender threats and fear that motivate protective security behaviors. *MIS Quarterly (MISQ)*, 39(4):837–864, 2015.

[25] J. C. Brancheau, B. D. Janz, and J. C. Wetherbe. Key issues in information systems management: 1994-95 SIM Delphi results. *MIS Quarterly*, 20(2):225–242, 1996.

[26] J. W. Brehm. Postdecision changes in the desirability of alternatives. *The Journal of Abnormal and Social Psychology*, 52(3):384–389, 1956.

[27] T. J. Brennan. Discounting the future: economics and ethics. In *The RFF Reader in Environmental and Resource Policy*, pages 48–54. Routledge, 2010.

[28] P. Bright. 2016 sees Internet Explorer usage collapse, Chrome surge, 2017. 7 January. Retrieved 29 Sept 2018 from: `https://arstechnica.com/information-technology/2017/01/2016-on-the-web-firefox-fights-back-as-microsofts-share-slumps/`.

[29] S. A. Buetow. Unsolicited GP advice against smoking: To give or not to give? *Journal of Health Communication*, 4(1):67–74, 1999.

[30] E. Burke. *Reflections on the Revolution in France and Other Writings*, volume 365. Everyman's Library, Cambridge, UK, 2015.

[31] A. Burton-Jones, E. R. McLean, and E. Monod. Theoretical perspectives in IS research: from variance and process to conceptual latitude and conceptual fit. *European Journal of Information Systems*, 24(6):664–679, 2015.

[32] B. M. Byrne. *Structural equation modeling with AMOS: Basic concepts, applications, and programming*. Routledge, New York, NY, 2016.

[33] Z. S. Byrne, K. J. Dvorak, J. M. Peters, I. Ray, A. Howe, and D. Sanchez. From the user's perspective: Perceptions of risk relative to benefit associated with using the internet. *Computers in Human Behavior*, 59:456–468, 2016.

[34] Z. Carmon and D. Ariely. Focusing on the forgone: How value can appear so different to buyers and sellers. *Journal of Consumer Research*, 27(3):360–370, 2000.

[35] P. Chatterjee, C. Irmak, and R. L. Rose. The endowment effect as self-enhancement in response to threat. *Journal of Consumer Research*, 40(3):460–476, 2013.

[36] R. Chung and D. F. Galletta. Genetic Basis of Behavioral Security. In *Proceedings of the Twelfth Annual Workshop on HCI Research in Management Information Systems, Milan, Italy, December*, volume 15, pages 9–13, 2013.

[37] R. B. Cialdini, M. R. Trost, and J. T. Newsom. Preference for consistency: The development of a valid measure and the discovery of surprising behavioral implications. *Journal of Personality and Social Psychology*, 69(2):318–328, 1995.

[38] D. K. Clark. The city government's role in community health improvement. *Public Health Reports*, 115(2-3):216–221, 2000.

[39] L. Coventry, P. Briggs, J. Blythe, and M. Tran. Using behavioural insights to improve the public's use of cyber security best practices, 2014. GOV.UK report, Government Office for Science. Retrieved 7 August 2018 from: `https://www.gov.uk/government/publications/cyber-security-using-behavioural-insights-to-keep-people-safe-online`.

[40] S. Creese, D. Hodges, S. Jamison-Powell, and M. Whitty. Relationships between password choices, perceptions of risk and security expertise. In *International Conference on Human Aspects of Information Security, Privacy, and Trust*, pages 80–89. Springer, 2013.

[41] M. L. Crossley. Introduction to the symposium 'Health Resistance': The limits of contemporary health promotion. *Health Education Journal*, 61(2):101–112, 2002.

[42] M. J. Culnan and P. K. Armstrong. Information privacy concerns, procedural fairness, and impersonal trust: An empirical investigation. *Organization Science*, 10(1):104–115, 1999.

[43] Cyber Essentials. Retrieved 2 June 2018 from: `http://www.cyberessentials.org`.

[44] J. D'Arcy, A. Hovav, and D. Galletta. User awareness of security countermeasures and its impact on information systems misuse: A deterrence approach. *Information Systems Research*, 20(1):79–98, 2009.

[45] E. L. Deci and R. M. Ryan. Self-determination theory. *Handbook of Theories of Social Psychology*, 1:416–433, 2011.

[46] N. Dhingra, Z. Gorn, A. Kener, and J. Dana. The default pull: An experimental demonstration of subtle default effects on preferences. *Judgment and Decision Making*, 7(1):69–76, 2012.

[47] T. Dinev and P. Hart. An extended privacy calculus model for e-commerce transactions. *Information Systems Research*, 17(1):61–80, 2006.

[48] G. B. Duggan, H. Johnson, and B. Grawemeyer. Rational security: Modelling everyday password use. *International Journal of Human-Computer Studies*, 70(6):415–431, 2012.

[49] C. Duhigg. *The Power of Habit: Why we do what we do and how to change*. William Heinemann, London, U.K., 2013.

[50] D. Y. Dupont and G. S. Lee. The endowment effect, status quo bias and loss aversion: Rational alternative explanation. *Journal of Risk and Uncertainty*, 25(1):87–101, 2002.

[51] S. Egelman, A. Sotirakopoulos, I. Muslukhov, K. Beznosov, and C. Herley. Does my password go up to eleven?: the impact of password meters on password selection. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, pages 2379–2388. ACM, 2013.

[52] S. Eidelman and C. S. Crandall. Bias in favor of the Status Quo. *Social and Personality Psychology Compass*, 6(3):270–281, 2012.

[53] D. Erdley. Computer hack cost Pennsylvania's Senate Democrats $700,000; others pay less-costly ransoms, 2018. Sept. 22. Retrieved 29 Sept 2018 from: `https://triblive.com/state/pennsylvania/14107828-74/computer-hack-cost-pennsylvanias-senate-democrats-700000-others-pay-less-costly-ransoms`.

[54] T. Eyal, N. Liberman, and Y. Trope. Judging near and distant virtue and vice. *Journal of Experimental Social Psychology*, 44(4):1204–1209, 2008.

[55] A. Farooq, J. Isoaho, S. Virtanen, and J. Isoaho. Information security awareness in educational institution: An analysis of students' individual factors. In *Trustcom/BigDataSE/ISPA, 2015 IEEE*, volume 1, pages 352–359, 2015.

[56] L. Festinger. *A theory of cognitive dissonance*, volume 2. Stanford University Press, 1962.

[57] M. L. Finucane and J. L. Holup. Risk as value: Combining affect and analysis in risk judgments. *Journal of Risk Research*, 9(2):141–164, 2006.

[58] G. J. Fitzsimons and D. R. Lehmann. Reactance to recommendations: When unsolicited advice yields contrary responses. *Marketing Science*, 23(1):82–94, 2004.

[59] R. Franciosi, P. Kujal, R. Michelitsch, V. Smith, and G. Deng. Experimental tests of the endowment effect. *Journal of Economic Behavior & Organization*, 30(2):213–226, 1996.

[60] L. P. Frankel and K. L. Otazo. Employee coaching: The way to gain commitment, not just compliance. *Employment Relations Today*, 19(3):311–320, 1992.

[61] K. Fujita, Y. Trope, N. Liberman, and M. Levin-Sagi. Construal levels and self-control. *Journal of Personality and Social Psychology*, 90(3):351–367, 2006.

[62] S. Furman, M. F. Theofanos, Y.-Y. Choong, and B. Stanton. Basing cybersecurity training on user perceptions. *IEEE Security and Privacy*, 10(2):40–49, Mar. 2012.

[63] S. Furnell. Assessing website password practices–over a decade of progress? *Computer Fraud & Security*, 2018(7):6–13, 2018.

[64] B. Gardner and C. Abraham. What drives car use? A grounded theory analysis of commuters' reasons for driving. *Transportation Research Part F: Traffic Psychology and Behaviour*, 10(3):187–200, 2007.

[65] B. Gardner, P. Lally, and J. Wardle. Making health habitual: the psychology of 'habit-formation' and general practice. *British Journal of General Practice*, 62(605):664–666, 2012.

[66] P. H. Gardner and D. C. Berry. The effect of different forms of advice on the control of a simulated complex system. *Applied Cognitive Psychology*, 9(7):S55–S79, 1995.

[67] V. Garg and J. Camp. End user perception of online risk under uncertainty. In *45th Hawaii International Conference on System Science (HICSS)*, pages 3278–3287. IEEE, 2012.

[68] J. Gaskin. Validity Master, Stats Tool Package, 2016. Retrieved 7 August 2018 from: https://www.scribd.com/document/81631601/Stats-Tools-Package.

[69] E. S. Geller. Evaluating energy conservation programs: Is verbal report enough? *Journal of Consumer Research*, 8(3):331–335, 1981.

[70] E. S. Geller, J. B. Erickson, and B. A. Buttram. Attempts to promote residential water conservation with educational, behavioral and engineering strategies. *Population and Environment*, 6(2):96–112, 1983.

[71] A. G. Greenwald. The totalitarian ego: Fabrication and revision of personal history. *American Psychologist*, 35(7):603–618, 1980.

[72] A. Hanamsagar, S. S. Woo, C. Kanich, and J. Mirkovic. Leveraging semantic transformation to investigate password habits and their causes. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*, page 570. ACM, 2018.

[73] Her Majesty's Government. Security features. Retrieved 2 June 2018 from: https://www.cyberaware.gov.uk/security-features.

[74] C. Herley. So long, and no thanks for the externalities: the rational rejection of security advice by users. In *Proceedings of the 2009 Workshop on New Security Paradigms Workshop*, pages 133–144. ACM, 2009.

[75] V. Hoorens, N. Remmers, and K. Van De Riet. Time is an amazingly variable amount of money: Endowment and ownership effects in the subjective value of working time. *Journal of Economic Psychology*, 20(4):383–405, 1999.

[76] C. Horne. Lack of cyber security knowledge leads to lazy decisions from executives. 2 November. Retrieved 2 June 2018 from: https://theconversation.com/lack-of-cyber-security-knowledge-leads-to-lazy-decisions-from-executives-68065, 2016.

[77] J. K. Horowitz and K. E. McConnell. A review of WTA/WTP studies. *Journal of Environmental Economics and Management*, 44(3):426–447, 2002.

[78] A. Hovav and J. D'Arcy. Applying an extended model of deterrence across cultures: An investigation of information systems misuse in the US and South Korea. *Information & Management*, 49(2):99–110, 2012.

[79] D.-L. Huang, P.-L. P. Rau, G. Salvendy, F. Gao, and J. Zhou. Factors affecting perception of information security and their impacts on it adoption and security practices. *International Journal of Human-Computer Studies*, 69(12):870–883, 2011.

[80] H. T. Hurt, K. Joseph, and C. D. Cook. Scales for the measurement of innovativeness. *Human Communication Research*, 4(1):58–65, 1977.

[81] B. Inder and T. O'Brien. The endowment effect and the role of uncertainty. *Bulletin of Economic Research*, 55(3):289–301, 2003.

[82] Information Commissioner's Office. A practical guide to IT security: ideal for the small business. Retrieved 2 June 2018 from `https://ico.org.uk/media/for-organisations/documents/1575/it_security_practical_guide.pdf`.

[83] M. Jakobsson. The human factor in phishing. *Privacy & Security of Consumer Information*, 7(1):1–19, 2007.

[84] W. James. *The Principles of Psychology*, volume 1. Dover Publications, New York, NY, 1890.

[85] R. Janoff-Bulman and S. S. Schwartzberg. Toward a general model of personal change. In C. Snyder and D. R. Forsyth, editors, *Handbook of Social and Clinical Psychology: The Health Perspective*, pages 488–508. Pergamon Press, 1991.

[86] T. Jefferson and R. Taplin. An investigation of the endowment effect using a factorial design. *Journal of Economic Psychology*, 32(6):899–907, 2011.

[87] A. C. Johnston and M. Warkentin. Fear appeals and information security behaviors: an empirical study. *MIS Quarterly*, 34(3):549–566, 2010.

[88] J. R. Jordan, H. R. Hungerford, and A. N. Tomera. Effects of two residential environmental workshops on high school students. *The Journal of Environmental Education*, 18(1):15–22, 1986.

[89] D. Kahneman, J. L. Knetsch, and R. H. Thaler. Experimental tests of the endowment effect and the Coase theorem. *Journal of Political Economy*, 98(6):1325–1348, 1990.

[90] D. Kahneman, J. L. Knetsch, and R. H. Thaler. Anomalies: The endowment effect, loss aversion, and Status Quo bias. *The Journal of Economic Perspectives*, 5(1):193–206, 1991.

[91] D. Kahneman and A. Tversky. Prospect theory: An analysis of decision under risk. *Econometrica: Journal of the Econometric Society*, 47(2):263–291, 1979.

[92] F. Kehr, T. Kowatsch, D. Wentzel, and E. Fleisch. Blissfully ignorant: the effects of general privacy concerns, general institutional trust, and affect in the privacy calculus. *Information Systems Journal*, 25(6):607–635, 2015.

[93] H.-W. Kim and A. Kankanhalli. Investigating user resistance to information systems implementation: a Status Quo bias perspective. *MIS Quarterly*, 33(3):567–582, 2009.

[94] I. Kirlappos and M. A. Sasse. Security education against phishing: A modest proposal for a major rethink. *IEEE Security & Privacy*, 10(2):24–32, 2012.

[95] T. Klaus and J. E. Blanton. User resistance determinants and the psychological contract in enterprise system implementations. *European Journal of Information Systems*, 19(6):625–636, 2010.

[96] J. L. Knetsch. The endowment effect and evidence of nonreversible indifference curves. *The American Economic Review*, 79(5):1277–1284, 1989.

[97] J. L. Knetsch and J. A. Sinden. Willingness to pay and compensation demanded: Experimental evidence of an unexpected disparity in measures of value. *The Quarterly Journal of Economics*, 99(3):507–521, 1984.

[98] H. Kruger, L. Drevin, and T. Steyn. A vocabulary test to assess information security awareness. *Information Management & Computer Security*, 18(5):316–327, 2010.

[99] L. Lapointe and S. Rivard. A multilevel model of resistance to information technology implementation. *MIS Quarterly*, pages 461–491, 2005.

[100] S. Laumer and A. Eckhardt. Why do people reject technologies: a review of user resistance theories. In *Information Systems Theory*, pages 63–86. Springer, 2012.

[101] J. S. Lerner, D. A. Small, and G. Loewenstein. Heart strings and purse strings: Carryover effects of emotions on economic decisions. *Psychological Science*, 15(5):337–341, 2004.

[102] K. Lewin. Frontiers in group dynamics: Concept, method and reality in social science; equilibrium and social change. *Human Relations*, 1(1):5–41, 1997.

[103] H. Liang and Y. Xue. Understanding security behaviors in personal computer usage: A threat avoidance perspective. *Journal of the Association for Information Systems*, 11(7):394–413, 2010.

[104] M. Limayem and S. G. Hirt. Force of habit and information systems usage: Theory and initial validation. *Journal of the Association for Information Systems*, 4(1):65–87, 2003.

[105] B. Lorenz, K. Kikkas, and A. Klooster. "The Four Most-Used Passwords Are Love, Sex, Secret, and God": Password Security and Training in Different User Groups. In *International Conference on Human Aspects of Information Security, Privacy, and Trust*, pages 276–283. Springer, 2013.

[106] M. L. Markus. Power, politics, and MIS implementation. *Communications of the ACM*, 26(6):430–444, 1983.

[107] M. L. Markus and D. Robey. Information technology and organizational change: causal structure in theory and research. *Management Science*, 34(5):583–598, 1988.

[108] L. E. Marsh, P. Kanngiesser, and B. Hood. When and how does labour lead to love? The ontogeny and mechanisms of the IKEA effect. *Cognition*, 170:245–253, 2018.

[109] M. J. Martinko, R. W. Zmud, and J. W. Henry. An attributional explanation of individual resistance to the introduction of information technologies in the workplace. *Behaviour & Information Technology*, 15(5):313–330, 1996.

[110] A. McCluskey and M. Lovarini. Providing education on evidence-based practice improved knowledge but did not change behaviour: a before and after study. *BMC Medical Education*, 5(1):40 (12 pages), 2005.

[111] D. McKenzie-Mohr. *Fostering sustainable behavior: An introduction to community-based social marketing*. New Society Publishers, Gabriola Island, Canada, 2013.

[112] P. Menard, M. Warkentin, and P. B. Lowry. The impact of collectivism and psychological ownership on protection motivation: A cross-cultural examination. *Computers & Security*, 75:147–166, 2018.

[113] J. Meyerhoff and U. Liebe. Status quo effect in choice experiments: empirical evidence on attitudes and choice task complexity. *Land Economics*, 85(3):515–528, 2009.

[114] C. J. Midden, J. F. Meter, M. H. Weenig, and H. J. Zieverink. Using feedback, reinforcement and information to reduce energy consumption in households: A field-experiment. *Journal of Economic Psychology*, 3(1):65–86, 1983.

[115] D. T. Miller and M. Ross. Self-serving biases in the attribution of causality: Fact or fiction? *Psychological Bulletin*, 82(2):213–225, 1975.

[116] D. Mochon, M. I. Norton, and D. Ariely. Bolstering and restoring feelings of competence via the IKEA effect. *International Journal of Research in Marketing*, 29(4):363–369, 2012.

[117] C. K. Morewedge and C. E. Giblin. Explanations of the endowment effect: an integrative review. *Trends in Cognitive Sciences*, 19(6):339–348, 2015.

[118] C. K. Morewedge, L. L. Shu, D. T. Gilbert, and T. D. Wilson. Bad riddance or good rubbish? Ownership and not loss aversion causes the endowment effect. *Journal of Experimental Social Psychology*, 45(4):947–951, 2009.

[119] S. Muehlbacher and E. Kirchler. Origin of endowments in public good games: The impact of effort on contributions. *Journal of Neuroscience, Psychology, and Economics*, 2(1):59–67, 2009.

[120] National Cyber Security Centre. 10 steps to cyber security, 2015. Retrieved 2 June 2018 from: `https://www.ncsc.gov.uk/guidance/10-steps-cyber-security`.

[121] D. Nayakankuppam and H. Mishra. The endowment effect: Rose-tinted and dark-tinted glasses. *Journal of Consumer Research*, 32(3):390–395, 2005.

[122] D. T. Neal, W. Wood, and A. Drolet. How do people adhere to goals when willpower is low? The profits (and pitfalls) of strong habits. *Journal of Personality and Social Psychology*, 104(6):959–975, 2013.

[123] J. C. Norcross, P. M. Krebs, and J. O. Prochaska. Stages of change. *Journal of Clinical Psychology*, 67(2):143–154, 2011.

[124] M. I. Norton, D. Mochon, and D. Ariely. The 'IKEA effect': When labor leads to love. *Harvard Business School Marketing Unit Working Paper*, 11(091), 2011.

[125] G. Ortona and F. Scacciati. New experiments on the endowment effect. *Journal of Economic Psychology*, 13(2):277–296, 1992.

[126] M. Osman, Y. Lin, and R. Ashcroft. Nudging: A lesson in the theatrics of choice. *Basic and Applied Social Psychology*, 39(6):311–316, 2017.

[127] A. S. Patrick, A. C. Long, and S. Flinn. HCI and Security Systems. In *CHI'03 Extended Abstracts on Human Factors in Computing Systems*, pages 1056–1057. ACM, 2003.

[128] J. Peck and S. B. Shu. The effect of mere touch on perceived ownership. *Journal of Consumer Research*, 36(3):434–447, 2009.

[129] A. Petru. Can companies restore consumer confidence after a data breach?, 2014. Security Magazine, Jul 8. Retrieved 29 Sept 2018 from: `https://www.triplepundit.com/special/internet-security/can-companies-restore-consumer-confidence-data-breach/`.

[130] S. K. Piderit. Rethinking resistance and recognizing ambivalence: A multidimensional view of attitudes toward an organizational change. *Academy of Management Review*, 25(4):783–794, 2000.

[131] C. Pinder, J. Vermeulen, B. R. Cowan, and R. Beale. Digital Behaviour Change Interventions to Break and Form Habits. *ACM Transactions on Computer-Human Interaction (TOCHI)*, 25(3):15:1–15:66, 2018.

[132] G. L. Polites and E. Karahanna. Shackled to the status quo: The inhibiting effects of incumbent system habit, switching costs, and inertia on new system acceptance. *MIS Quarterly*, 36(1):21–42, 2012.

[133] A. Prestwich, M. Perugini, R. Hurling, and J. Richetin. Using the self to change implicit attitudes. *European Journal of Social Psychology*, 40(1):61–71, 2010.

[134] J. O. Prochaska and W. F. Velicer. The transtheoretical model of health behavior change. *American Journal of Health Promotion*, 12(1):38–48, 1997.

[135] C. A. Quinsey. Time for a HIPAA Tune-Up?: Penalties Now in Effect for Noncompliance. *Journal of AHIMA*, 77(5):64–65, 2006.

[136] A. E. Rafferty, N. L. Jimmieson, and A. A. Armenakis. Change readiness: A multilevel review. *Journal of Management*, 39(1):110–135, 2013.

[137] J. Reb and T. Connolly. Possession, feelings of ownership and the endowment effect. *Judgment and Decision Making*, 2(2):107–114, 2007.

[138] E. M. Redmiles, S. Kross, and M. L. Mazurek. How I Learned to Be Secure: A Census-Representative Survey of Security Advice Sources and Behavior. In *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, CCS '16, pages 666–677, 2016.

[139] K. Renaud. Blaming noncompliance is too convenient: What really causes information breaches? *IEEE Security & Privacy*, 10(3):57–63, 2012.

[140] K. Renaud. How smaller businesses struggle with security advice. *Computer Fraud & Security*, 2016(8):10–18, 2016.

[141] K. Renaud, S. Flowerday, M. Warkentin, P. Cockshott, and C. Orgeron. Is the responsibilization of cyber security risk reasonable and judicious? *Computers & Security*, 78:198–211, 2018.

[142] K. Renaud and M. Warkentin. Risk Homeostasis in Information Security: Challenges in Confirming Existence and Verifying Impact. In *Proceedings of the New Security Paradigms Workshop*, pages 57–69. ACM, 2017.

[143] K. Renaud and M. Warkentin. Using Intervention Mapping to Breach the Cyber-Defense Deficit. In *12th Annual Symposium on Information Assurance (ASIA '17) June 7-8*, Empire State Plaza in Albany, NY, 2017.

[144] K. Renaud and V. Zimmermann. Nudging folks towards stronger password choices: providing certainty is the key. *Behavioural Public Policy*, pages 1–31, 2018.

[145] A. Schurr and I. Ritov. The effect of giving it all up on valuation: A new look at the endowment effect. *Management Science*, 60(3):628–637, 2013.

[146] Scottish Business Resilience Centre. Cyber Security Resources. Retrieved 2 June 2018 from: `www.sbrcentre.co.uk/resources`.

[147] K. E. See, E. W. Morrison, N. B. Rothman, and J. B. Soll. The detrimental effects of power on confidence, advice taking, and accuracy. *Organizational Behavior and Human Decision Processes*, 116(2):272–285, 2011.

[148] T. Sharot, C. M. Velasquez, and R. J. Dolan. Do decisions shape preference? Evidence from blind choice. *Psychological Science*, 21(9):1231–1235, 2010.

[149] T. Shavit, D. Sonsino, and U. Benzion. On the evaluation of options on lotteries: An experimental study. *The Journal of Psychology and Financial Markets*, 3(3):168–181, 2002.

[150] D. K. Sherman and G. L. Cohen. The psychology of self-defense: Self-affirmation theory. *Advances in Experimental Social Psychology*, 38:183–242, 2006.

[151] J. Shropshire, M. Warkentin, and S. Sharma. Personality, attitudes, and intentions: Predicting initial adoption of information security behavior. *Computers & Security*, 49:177–191, 2015.

[152] S. B. Shu and J. Peck. Psychological ownership and affective reaction: Emotional attachment process variables and the endowment effect. *Journal of Consumer Psychology*, 21(4):439–452, 2011.

[153] R. C. Solomon. Envy and resentment: Corporate poison. In *Ethics and Excellence, The Ruffin Series in Business Ethics*, chapter 23, pages 242–245. Oxford University Press, New York, USA, 1993.

[154] E. H. Spafford. OPUS: Preventing weak password choices. *Computers & Security*, 11(3):273–278, 1992.

[155] M. A. Strahilevitz and G. Loewenstein. The effect of ownership history on the valuation of objects. *Journal of Consumer Research*, 25(3):276–289, 1998.

[156] D. W. Straub and R. J. Welke. Coping with systems risk: security planning models for management decision making. *MIS Quarterly*, 22(4):441–469, 1998.

[157] K. Sweeny, D. Melnyk, W. Miller, and J. A. Shepperd. Information avoidance: Who, what, when, and why. *Review of General Psychology*, 14(4):340–353, 2010.

[158] S. E. Taylor. Adjustment to threatening events: A theory of cognitive adaptation. *American Psychologist*, 38(11):1161–1173, 1983.

[159] M. Thomson, D. J. MacInnis, and C. Whan Park. The ties that bind: Measuring the strength of consumers' emotional attachments to brands. *Journal of Consumer Psychology*, 15(1):77–91, 2005.

[160] L. K. Trevino. Experimental approaches to studying ethical-unethical behavior in organizations. *Business Ethics Quarterly*, 2(2):121–136, 1992.

[161] B. Trinkle, R. E. Crossler, and M. Warkentin. I'm game, are you? Reducing real-world security threats by managing employee activity in virtual environments. *Journal of Information Systems*, 28(2):307–327, 2014.

[162] Y. Trope and N. Liberman. Construal-level theory of psychological distance. *Psychological Review*, 117(2):440–463, 2010.

[163] Y. Trope, N. Liberman, and C. Wakslak. Construal levels and psychological distance: Effects on representation, prediction, evaluation, and behavior. *Journal of Consumer Psychology*, 17(2):83–95, 2007.

[164] H.-y. S. Tsai, M. Jiang, S. Alhabash, R. LaRose, N. J. Rifon, and S. R. Cotten. Understanding online safety behaviors: A protection motivation theory perspective. *Computers & Security*, 59:138–150, 2016.

[165] A. Tsohou, M. Karyda, and S. Kokolakis. Analyzing the role of cognitive and cultural biases in the internalization of information security policies: recommendations for information security awareness programs. *Computers & Security*, 52:128–141, 2015.

[166] A. Tversky and D. Kahneman. Loss aversion in riskless choice: A reference-dependence model. *Quarterly Journal of Economics*, 106(4):1039–1061, 1991.

[167] N. van de Ven, M. Zeelenberg, and E. van Dijk. Buying and selling exchange goods: Outcome information, curiosity and the endowment effect. *Journal of Economic Psychology*, 26(3):459–468, 2005.

[168] L. Van Dyne and J. L. Pierce. Psychological ownership and feelings of possession: Three field studies predicting employee attitudes and organizational citizenship behavior. *Journal of Organizational Behavior*, 25(4):439–459, 2004.

[169] J. Van Niekerk and R. von Solms. A holistic framework for the fostering of an information security sub-culture in organizations. In *Information Security South Africa*, pages 1–13, Johannesburg, 2005. 29 June to 1 July.

[170] P. van Schaik, D. Jeske, J. Onibokun, L. Coventry, J. Jansen, and P. Kusev. Risk perceptions of cyber-security and precautionary behaviour. *Computers in Human Behavior*, 75:547–559, 2017.

[171] A. Vance, M. Siponen, and S. Pahnila. Motivating IS security compliance: insights from habit and protection motivation theory. *Information & Management*, 49(3):190–198, 2012.

[172] H. Varian. Managing online security risks, 2000. The New York Times, 1 June. Retrieved 19 Sept 2018 from: `https://archive.nytimes.com/www.nytimes.com/library/financial/columns/060100econ-scene.html`.

[173] W. K. Viscusi, W. A. Magat, and J. Huber. An investigation of the rationality of consumer valuations of multiple health risks. *The RAND Journal of Economics*, 18(4):465–479, 1987.

[174] P. Walla. Non-conscious brain processes revealed by Magnetoencephalography (MEG). In *Magnetoencephalography*, chapter 12, pages 235–252. `www.intechopen.com`, 2011. DOI: 10.5772/28211.

[175] B. N. Waller. Deep thinkers, cognitive misers, and moral responsibility. *Analysis*, 59(264):223–229, 1999.

[176] M. Warkentin, K. Davis, and E. Bekkering. Introducing the check-off password system (COPS): an advancement in user authentication methods and information security. *Journal of Organizational and End User Computing (JOEUC)*, 16(3):41–58, 2004.

[177] M. Warkentin, A. C. Johnston, and J. Shropshire. The influence of the informal social learning environment on information privacy policy compliance efficacy and intention. *European Journal of Information Systems*, 20(3):267–284, 2011.

[178] D. Whitehead and G. Russell. How effective are health education programmes—resistance, reactance, rationality and risk? Recommendations for effective practice. *International Journal of Nursing Studies*, 41(2):163–172, 2004.

[179] R. Willison and M. Warkentin. Beyond deterrence: An expanded view of employee computer abuse. *MIS Quarterly*, 37(1):1–20, 2013.

[180] R. Willison, M. Warkentin, and A. C. Johnston. Examining employee computer abuse intentions: Insights from justice, deterrence, and neutralization perspectives. *Information Systems Journal*, 28(2):266–293, 2018.

[181] C. C. Wood. Policies alone do not constitute a sufficient awareness effort. *Computer Fraud & Security*, 1997(12):14–19, 1997.

[182] W. Wood and D. T. Neal. A new look at habits and the habit-goal interface. *Psychological Review*, 114(4):843–863, 2007.

[183] M. Workman, W. H. Bommer, and D. Straub. Security lapses and the omission of information security measures: A threat control model and empirical test. *Computers in Human Behavior*, 24(6):2799–2816, 2008.

[184] J. Yan, S. Early, and R. Anderson. The XenoService —- A distributed defeat for distributed denial of service. In *Proceedings of the International Workshop on Information Security*, 2000. December 20–21. Wollongong, Australia.

[185] I. Yaniv. Receiving other people's advice: Influence and benefit. *Organizational Behavior and Human Decision Processes*, 93(1):1–13, 2004.

[186] I. Yaniv and E. Kleinberger. Advice taking in decision making: Egocentric discounting and reputation formation. *Organizational Behavior and Human Decision Processes*, 83(2):260–281, 2000.

[187] M. Zeelenberg and E. Van Dijk. A reverse sunk cost effect in risky decision making: Sometimes we have too much invested to gamble. *Journal of Economic Psychology*, 18(6):677–691, 1997.

[188] W. Zhang and P. Xu. Do I have to learn something new? Mental models and the acceptance of replacement technologies. *Behaviour & Information Technology*, 30(2):201–211, 2011.

[189] Y. Zhang and A. Fishbach. The role of anticipated emotions in the endowment effect. *Journal of Consumer Psychology*, 15(4):316–324, 2005.

[190] G. K. Zipf. *Human behavior and the principle of least effort: An introduction to human ecology*. Addison-Wesley, Cambridge, Massachussets, 1949.

Appendix: Endowment Calculus Causative Measures

Self-Image Test

Terry and Pat are talking about how they create their passwords. Terry's and Pat's ways of coming up with new passwords are very different.

Terry says to Pat: "Your way is just plain wrong!"

How do you think Pat reacts? Check as many as apply.

a) Pat retorts "My way is better than yours."

b) Pat says "My way is good enough."

c) Pat feels hurt.

d) Pat changes the subject.

e) Pat ends the conversation and walks away.

f) Pat says "Explain why it is wrong."

g) Pat says "Tell me more so I can adopt your way."

h) None of the above, please explain.

Over-Valuing Test

Imagine you are opening a new online banking account. You've just come to the part of the process where you're asked to provide a password to protect your account.

Come up with a NEW password in your mind. Don't reuse one of your other passwords.

Now think about the process you've just engaged in to come up with your new password and bear it in mind in answering the next few screens of questions

Imagine the bank really wants to encourage their customers to create stronger passwords. They are thinking of paying people hard cash to do this.

How much should the bank offer their customers (in US dollars) to create a stronger password for their account at this bank?

How much would the bank have to offer YOU personally (in US dollars) to create a stronger

password?

Measuring Endowment Causatives and Calculus Elements

(Capitalization exactly as used in Survey)

Ownership	**O1:** I feel a high degree of OWNERSHIP of my password creation strategy. **O2:** I feel like I OWN my password creation strategy. **O3:** I feel like the way I create passwords is "MY" password creation strategy.
Attachment	**A1:** **My** passwords protect my online accounts. **A2:** **My** passwords EFFECTIVELY protect **my** accounts. **A3:** I believe **my** password creation strategy is GOOD ENOUGH for me. **A4:** The passwords **I** use to protect IMPORTANT accounts are STRONG ENOUGH to resist attempts to breach them.
Perceived Risk	**P1:** **My** passwords are MORE LIKELY to protect me than passwords created using other routines. **P2:** The passwords I create are BETTER THAN alternatives created using other routines. **P3:** **My** password creation routine makes it HARDER FOR HACKERS to guess my passwords than other creation routines.
Change Willingness	**C1:** I am *willing to consider* CHANGING the way I create passwords. **C2:** I *plan* to CHANGE the way I create my passwords. **C3:** I *predict* that I will CHANGE the way I create my passwords.

Biographies

Karen Renaud is a Scottish computing Scientist working on all aspects of Human-Centred Security and Privacy. She is Professor of Cyber Security in the Division of Cyber Security at the University of Abertay in Dundee, Scotland. Karen holds a first class Masters degree in Computer Science from the University of South Africa, and a PhD from the University of Glasgow. Karen is particularly interested in deploying behavioural science techniques to improve security behaviours, and in encouraging end-user privacy-preserving behaviours. Her research approach is multi-disciplinary, essentially learning from other, more established, fields and harnessing methods and techniques from other disciplines to understand and influence cyber security behaviours. Karen was one of five UK Cyber Security Fulbright Awardees for 2016/17, hosted at Mississippi State University in Starkville, Mississippi in the USA. She is associate editor for the International Journal of Human Computer Studies, Transactions on Computer Forensics and Security, The Journal of Security and Applications and Information Technology & People.

Robert F. Otondo is an Associate Professor of Information Systems at Mississippi State University. He received his Ph.D. in Computer Information Systems at Arizona State University. His research interests center on perceptions and uses of emerging technologies. Dr. Otondo's research has been funded by the National Science Foundation, the Office of Naval Research, the Robert Wood Johnson Foundation, and the FedEx Center for Supply Chain Management at The University of Memphis. His research has been published in the European Journal of Information Systems, MIS Quarterly, Journal of Applied Psychology, Information & Management, Personnel Psychology, Human Relations, Production and Operations Management, and Decision Support Systems.

Merrill Warkentin is the James J. Rouse Professor of Information Systems in the College of Business at Mississippi State University. His primary research focus is in behavioral IS security and privacy issues, and has appeared in MIS Quarterly, Journal of MIS, Journal of the AIS, European Journal of Information Systems, Information Systems Journal, Decision Sciences, Information & Management, and others. He was the 2016 AMCIS Program Co-Chair. He holds or has held editorial positions at MIS Quarterly, Information Systems Research, European Journal of Information Systems, Decision Sciences, Information & Management, and the AIS Transactions on Replication Research.