Modeling inertia causatives: validating in the password manager adoption context

Karen Renaud
Jacques Ophoff

MODELING INERTIA CAUSATIVES; VALIDATING IN THE PASSWORD MANAGER ADOPTION CONTEXT

Karen Renaud[1] **and Jacques Ophoff**[2]
[1]University of Abertay, Dundee, U.K, [2]University of Cape Town, Cape Town, South Africa
k.renaud@abertay.ac.uk, jacques.ophoff@uct.ac.za

ABSTRACT

Cyber criminals are benefiting from the fact that people do not take the required precautions to protect their devices and communications. It is the equivalent of leaving their home's front door unlocked and unguarded, something no one would do. Many efforts are made by governments and other bodies to raise awareness, but this often seems to fall on deaf ears. People seem to resist changing their existing cyber security practices: they demonstrate *inertia*. Here, we propose a model and instrument for investigating the factors that contribute towards this phenomenon.

1 Introduction

The cyber crime field is a relatively new one, as compared to the centuries-old history of deviant human behaviors. That being so, many entities are working hard to raise awareness of the cyber risks, consequences and particularly the actions that people should take to protect themselves [6, 84, 43]. These security awareness and training drives seem to be enthusiastically received. Sometimes people express an intention to adopt the recommended behaviors. Yet such intentions do not always convert to actual behaviors [77, 2]. In many cases people seem to resist following the advice [41, 57]. Such resistance can be either active or passive [44] and might manifest as low levels of usage, by a refusal to use, or by dysfunctional use [51].

Resistance has been attributed to individual intransigence, stubbornness or moral weakness [22, 59, 83]. Yet attributing resistance to personal failings is unhelpful and unproductive. Wegener *et al.* [82] point out that a better understanding of resistance will help us to craft messages that might be more persuasive.

If we really want people to adopt security behaviors, we need to understand exactly what causes them to resist. With a more nuanced understanding, organizations will be in a better position to move people towards the desired actions. In this regard we propose the following **research question**: *"How does resistance to recommendations manifest itself in the behavioural information security domain?"* To investigate the resistance phenomenon we propose a model grounded in the status quo literature, with maintaining the status quo manifesting as inertia. Our model also investigates other biases that are possibly antecedents of inertia.

In Section 2 we explore the background literature on resistance and inertia. In Section 2.4 we also present the context (password manager adoption) within which we situate our investigation. Section 3 then proposes a model for inertia

in the cyber security context. In Section 4 we explain how we intend to validate the model in the password manager adoption context. Section 5 concludes.

2 Background

Security awareness and training drives address the so-called "knowledge gap" that undeniably exists within the cyber security domain. Yet it has become clear that even people with the requisite cyber knowledge do not always behave securely [32, 63].

Researchers attribute resistance to a failure to take responsibility for cybersecurity [74], poor system design [16, 30, 65, 61], carelessness [74], lack of ability [18] or stubbornness [71]. Other factors cited by researchers include people resisting because they know people are trying to convince them [35], anxiety about the consequences of the change, when there is mistrust of the people advocating a change and uncertainty avoidance [13, 14]. These explanations tend to reduce resistance to an individual pathology. Others consider the problem to be structural, with the problems manifesting as resistance being due to the way end users are perceived and treated: as a "problem" [87]. Here the prevalence of resistance is attributed to a more social pathology. It is more likely to have elements of both individual and social pathologies, and also be an artefact of the interaction between the individual and the system.

A perception that the problem is rooted in the individual leads to organizational responses with the same flavor, including redoubling efforts to improve compliance [9, 70, 80] or imposing penalties for non-compliance [34, 62]. These efforts could lead to resentment [11, 72] or disgruntlement [26] because they focus on the symptom and not on the cause. Many of the underlying resistance-triggering factors are invisible, yet observable inertia results. Donald [21] argues that resistance is a multi-dimensional concept and that our responses, too, ought to be multi-dimensional. As a first step, we should seek to understand the concept of resistance more clearly before we attempt to ameliorate the symptoms.

2.1 Defining and Understanding Resistance

Resistance is defined by the OED as "*The refusal to accept or comply with something*." In the cyber security context, this might mean that people resist adopting advised secure actions, or continue to behave insecurely. Knowles and Lin [42] explain that resistance can have three sources, as shown in Figure 1. Awareness drives only address the cognitive aspects, with compliance-related efforts being likely to exacerbate existing negative affective responses.

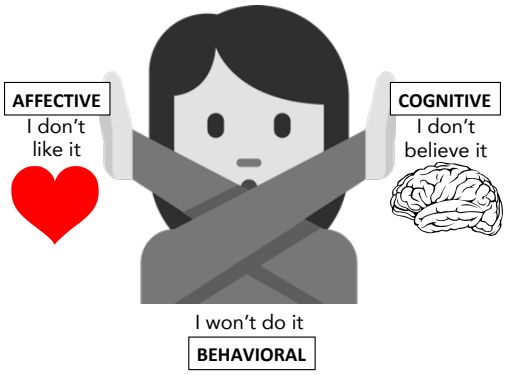

Figure 1: Sources of Resistance [42]

Laumer and Eckhardt [44] explain that people can react in a number of ways when they encounter a new technology. If they do not accept it, they might reject, resist or simply not adopt. Rejection, they define, as a refusal to engage with the technology at all, by dismissing it as faulty or inadequate. Resistance, on the other hand, means that they actively try to prevent its implementation. Non-adoption is defined as a deliberate and considered choice not to use the technology.

The parallels with the concepts depicted in Figure 1 are that the first of these is cognitive and affective, the second is cognitive, affective and behavioral, while the third is primarily cognitive. The act of resisting can have elements of both rejection and non-adoption [44]. Sometimes people prefer either to do nothing, or to continue with whatever practices they have been engaged in up to that point. This is the status quo bias that manifests as *inertia*.

Donald [21] argues that resistance is a multi-dimensional concept and that our responses, too, ought to be multi-dimensional. As a first step, we should seek to understand the concept of resistance more clearly before we attempt to ameliorate it when it manifests as inertia.

Resistance is clearly a complex phenomenon with many triggering factors. Doing it justice in a single paper is unrealistic. We have chosen to focus on one kind of resistance: inertia. This has been a relatively poorly studied phenomenon [60], and, to our knowledge, not yet studied in the cybersecurity context.

2.2 Relevant Biases

Samuelson and Zeckhauser [69] explain that the status quo bias causes a tendency towards "*doing nothing or maintaining one's current or previous decision*" [p. 7] i.e. inertia. This might have less to do with the perceived quality of the existing routine, or be rooted in the fact that the person, him or herself, who has formulated the routine. Researchers have identified a number of status-quo related factors: a preference for the familiar [35], mistrust [13], uncertainty [15, 39], sunk costs [39], past negative experiences [15], switching costs [40, 39, 60, 60], IT anxiety [10], social influence [23], personal values [17], threats to something the person cares about [31] and the influence of habit [60]. This could well explain a reluctance to make any changes at all in how people manage their passwords.

Polites and Karahanna [60] define inertia as "*attachment to, and persistence of, existing behavior patterns*" [p.24]. They also argue that three particular mediators exist to make people tend towards inertia: *rationalizations*, *psychological commitment* and *cognitive misperceptions*. Figure 2 shows how these three aspects align with the concepts in Figure 1.

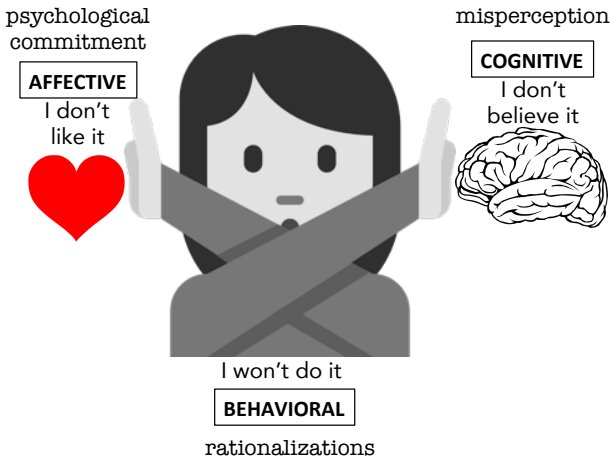

Figure 2: Inertia Antecedents

There are two biases that align with Polites and Karahanna's notion of attachment to the person's existing practice or routine: (1) the endowment effect [36] and (2) the IKEA effect [58].

The Endowment Effect: This effect leads people to be overly attached to, and over-value, something they *own*. Renaud *et al.* [64] investigated the influence of the *endowment effect* on password creation routines. They found that people were attached to their existing routines and this led them to resist persuasive attempts to adopt a new routine.

The IKEA Effect: The IKEA effect [58] is characterized by people taking *pride* in things they create, and then becoming attached to them. This might also apply to people's pre-existing security routines if they came up with it themselves and feel a sense of pride in their self-made solution to the conundrum.

Difference: With the endowment effect, people *actively* over value their existing routine and justify their preference for it by considering it better than the proposed alternative. The IKEA effect is slightly different. Here the person personally creates their existing routine, and feels proud of it. Endowment, on the other hand, only requires ownership to trigger, not self creation or pride. We do not suggest that these biases are independent; they could co-exist and exert different levels of influence on a person who is being confronted with a persuasive message.

A cross-cutting bias that probably plays a role in encouraging all these effects is the confirmation bias [56]. This effect suggests that people seek out evidence to confirm their existing beliefs and validates their existing choices. This might play a role in the triggering of the endowment, IKEA and status quo biases.

2.3 Inertia as Outcome

Resistance is not a purely negative phenomenon, but can also be a positive phenomenon, especially when people question the wisdom of the advised course of action, and reveal flaws in the persuasive argument [82]. Zandvoort [85] claims that the ability to resist is essential in allowing people to develop stable self identities. Wegener *et al.* [82] also argue that a measure of resistance ought to be fostered to ensure that people resist attempts to move them away from their current advisable course of action. Apart from self actualization, as argued by [85], there are also other benefits of declining to change. For example Alós-Ferrer *et al.* [5] found that decisions are slower when people had to decide between their usual routine and a new optimal routine. Moreover, they argue that inertia aligns with the human preference for consistency [47] and desire for the familiar [35].

However, inertia in cybersecurity is a matter of concern because it might well prevent people from adopting secure behaviors. As such, we need to understand the triggering factors so that we can attempt to alleviate them. In the next section, we outline a design of a study to explore these factors. We will focus primarily on the *status quo* bias and IKEA effect factors, because the endowment effect has already been widely studied and is well understood.

To ensure that the questions we pose in the study are reasonable, we have to choose one particular context; an area where people are likely to have pre-existing behaviors. The obvious choice is passwords, and the persuasive message we chose is that of password managers. This is an interesting context because password managers are not widely adopted [66], for various reasons [3, 4, 50].

2.4 Study Context

To study the effects of user resistance and inertia in the information security domain a task needs to be selected. There should be more than one way of completing the task (i.e. 'an incumbent vs. new system') and both should be available for use. Thus use of the new system should not be mandated and the incumbent system will not be discontinued [60], giving people the choice to accept or resist the new system. Considering the above requirements, the task chosen in this study is the *individual management of passwords for online accounts*. Multiple systems exist to manage passwords, including manual memory-based routines as well as software-based personal password managers.

Authentication by password is the most common method used to protect user accounts online. While passwords are an important part of protecting users' information assets and resources, they are vulnerable to social engineering and hacking attacks [38]. Weak passwords that are easy to guess, or hack by password cracking tools, increase users' vulnerability to threats [76, 78]. Despite the clear risk of using a weak password, users nevertheless persist in using insecure passwords that are easy to guess and hack. Strong passwords are difficult to remember, with users struggling to recall and therefore recycling passwords [25, 81]. Such poor practices also occur because users find it inconvenient to comply with inconsistent password requirements [54].

To assist users, additional feedback mechanisms, such as password strength meters, are sometimes used to motivate stronger passwords [78]. The results show implementation nuances [75], while another problem is the infrequent use of such mechanisms across websites. Therefore, attention has been called "to better support the use of passwords" [30]. One form of support is personal password managers.

Password managers are "*programs used to generate, encrypt, and store passwords for a client-side user*" [49]. Password managers make use of a master password to unlock a database of more complex passwords, decreasing the cognitive burden of users [48, 86]. It is accepted that password managers "remove the effort from password management" [3]. Use of password managers allow users to generate complex passwords with high entropy, based on either the general settings supplied by the program or by using custom character sets.

Fagan *et al.* [24] note that the purpose of password managers is often misunderstood by both users and non-users alike. Examining user considerations in the adoption of password managers show that convenience and usefulness are important factors, while security concerns are cited by users that do not use such tools [24]. While password managers are well established, concerns include susceptibility of the password manager's database to attacks [28] as well as the possibility of data exfiltration during use [48]. Despite these concerns, from an emotional perspective users of password managers are "*likely to feel secure, admiring and energetic, and less likely to feel suspicious when using their password manager to log into a website*" [24]. Arguably password managers offer the ability to generate more secure passwords and manage them in an efficient way. Thus, the average user would benefit by switching from a manual password routine to the use of a personal password manager. This switch need not happen for all of a user's accounts but is preferable for accounts that store valuable and sensitive user information.

3 Model Proposal

Previous studies have used several technology acceptance models to investigate the effects of user resistance and inertia. An essential requirement of a theory that attempts to models password manager adoption is that it has to acknowledge that people have pre-existing password management routines. Any model of password manager adoption must take cognisance of the fact that such adoption *replaces* current password management routines [64]. Any theory modeling password manager adoption has to include some notion of existing practice. Lebek *et al.* [45] carried out a theory-based review of information security related research. They mention the most often used theories in the information security domain: the Theory of Reasoned Action [29], the Theory of Planned Behaviour (TPB) [1], General Deterrence Theory (GDT) [55], Protection Motivation Theory (PMT) [68], the Technology Acceptance Model (TAM) [19], Social Cognitive Theory (SCT) [7], Constructivism [27] and Social Learning Theory (SLT) [8].

SLT and constructivism are learning theories, so do not qualify. GDT, reflecting deterrence, is also unsuitable for this adoption context. The rest do not incorporate any notion of a pre-existing practice. Hence, none of these is a good fit for modeling password manager adoption. Hence we chose to extend one of these models to incorporate pre-existing practice, while retaining the constructs that have been shown to influence inertia.

We extended the TAM model [20] with the subjective norm, which is conceptually similar to Polites and Karahanna's inertia model [60]. TAM includes perceived usefulness (PU), perceived ease of use (PEOU), and usage intention. Since our new system is proposed as a replacement for a manual password routine we use relative advantage (RA) instead of PU [67]. The relationships between these constructs are not the focus of our research, but have been theoretically justified in prior studies; we thus do not formally hypothesise them. We present our conceptual model in Figure 3. The core of the model (right-hand box) represents an individual's behavioural and normative beliefs and intentions toward using a new system. *In our study, the new system is conceptualised as a personal password manager.*

We extend (left-hand box) the core model with constructs associated with the incumbent system, defined as *a user's manual password routine*. These constructs focus on inertia as a manifestation of status quo bias [60]. We add three conscious sources of inertia, namely perceived transition costs, sunk costs, and IKEA effect. While transition costs

evaluate the effort of switching to the new system [40], sunk costs and the IKEA effect represent the effort invested into the incumbent system as value, thus justifying remaining with the *status quo* [33].

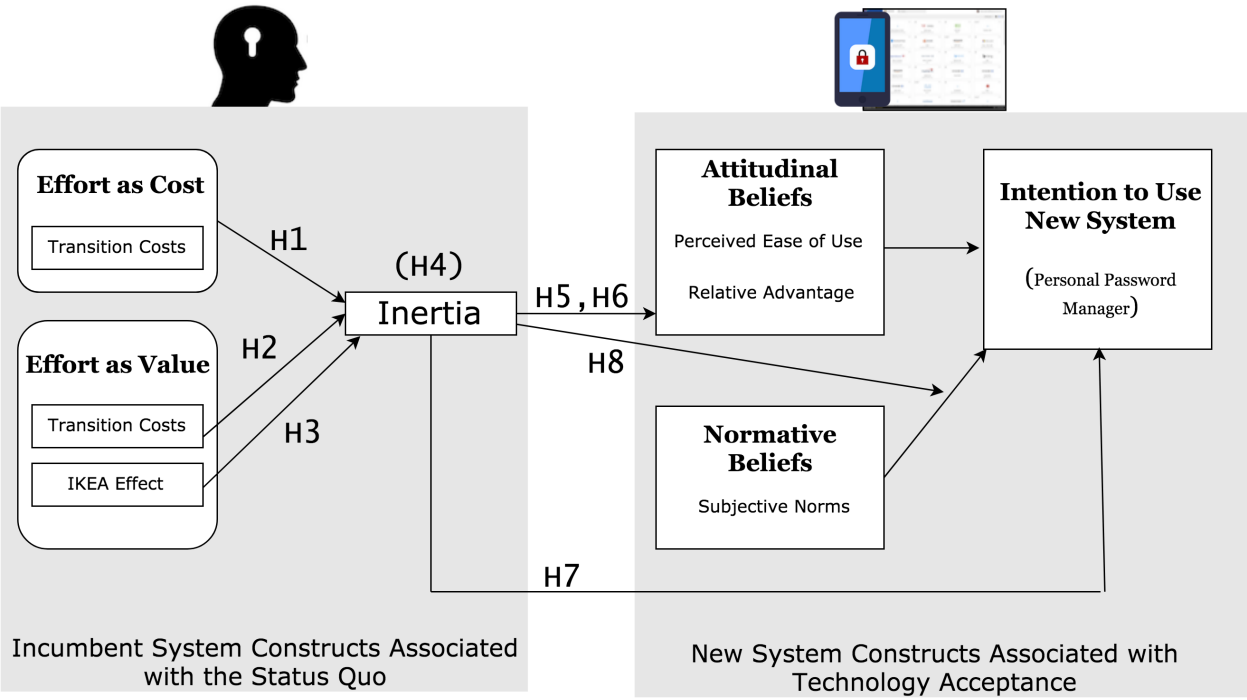

Figure 3: Conceptual Model

3.1 Inertia and Perceived Costs of Switching from the Status Quo

Research has conceptualised inertia to be a result of conscious bias toward the status quo [60]. In this research we focus our attention on effort and its influence on inertia, as informed by status quo bias and IKEA effect. First, it should be noted that effort is conceptually different to motivation. Effort can be defined as "*intensification of either mental or physical activity in the service of meeting some goal*", whereas motivation is "*a (psychological) force that drives behaviour and that consists of a direction (e.g., a goal) and an intensity or amplitude with which this direction is pursued (i.e., effort).*" [33] While a large amount of information security research has focused on the constructs and processes related to motivation (e.g. [34, 12]), effort is a rather less-explored concept.

Traditionally effort has been seen as costly and something to avoid. An explanation which ties in with status quo bias is *rational decision making* based on assessing transition costs. Common costs include the time and effort required to learn how to use the new system. Such costs mean a switch from the status quo is less likely [69]. Thus, we expect that when users perceive the time and effort required to learn how to use a personal password manager as high this will result in a greater level of inertia and sticking with their current manual password routine. Thus, we propose:

Hypothesis 1 *Perceived transition costs will positively impact inertia.*

Despite clear evidence of effort's costs, it has also been argued that effort adds value, both to the resulting goal and the activity itself [33]. Two theories related to effort's perceived value are incorporated into our model: the sunk costs and IKEA effect. These explanations leverage status quo bias by explaining that the status quo is maintained because of *psychological commitment* to an existing course of action [69].

Sunk costs reflect the fact that users are more likely to continue using an option the more effort has already been invested into it [33]. Thus, a course of action is justified based on previous commitments (good or bad) to that action [60]. Sunk costs related to technology can include the time and effort already invested into the incumbent system, as well as "*skills related to the previous way of working (which will be lost as a result of switching)*" [40]. Based on this we expect that users who perceive an existing investment of time and effort into their current password routine will exhibit higher levels of inertia. Thus, we propose:

Hypothesis 2 *Perceived sunk costs will positively impact inertia.*

The IKEA effect suggests that effort by itself can induce greater liking for the resulting product [58]. Put another way, users value products they successfully create themselves more than identical products that are ready-made (by others). A possible explanation for this effect is that it justifies in part the effort that has already been exerted (effort justification) [33]. Research has also shown that the effect is based on feelings of competence, reflected through pride in the resulting product [52]. We expect users who perceive themselves as competent at their current password routines to show higher levels of inertia, and to be less likely to switch from the status quo. Thus, we propose:

Hypothesis 3 *The IKEA effect will positively impact inertia.*

3.2 The Influence of Inertia on New System Acceptance

It has been shown that inertia is an important mechanism through which perceptions of switching costs (e.g. sunk costs) impact technology acceptance [60]. In keeping with previous research we expect perceived transition costs, sunk costs, and the IKEA effect to impact PEOU and RA of the new system, by biasing the user towards the status quo (causing inertia). While it is proposed that "*in the presence of known alternatives, transition costs could have direct effects on perceived usefulness and perceive ease of use, in addition to the indirect effect through inertia*" [60] there is currently no evidence to support this view. We propose that inertia plays a mediating role between the incumbent system constructs and beliefs about the new system, as follows:

Hypothesis 4 *Inertia will fully mediate the relationships between the incumbent system constructs of transition costs, sunk costs, and IKEA effect and the new system technology acceptance constructs.*

3.3 The Impact of Inertia on Intention

Findings from previous research support several possible effects of inertia on the intention to use the new system [60]. First, inertia may negatively impact perception of PEOU and RA of the new system. Inertia has a mediating effect and negatively biases users' beliefs about the new system, resulting in lower intentions to use it. This view is also supported by status quo bias through various theories (e.g. self perception theory, cognitive dissonance, etc.). By relying on past behaviour, users may avoid making an accurate comparison between the incumbent and new system [69]. If a user doesn't want to give up their current way of doing things, they may also try to justify their actions to maintain cognitive consistency; "*an inert user of an incumbent system to bias their perceptions of a new system downward to eliminate cognitive dissonance and continue in the status quo*." [60] Thus a lack of motivation for change will manifest as lowered perceptions of new system benefits. Thus, we propose:

Hypothesis 5 *Inertia will negatively impact perceptions of the ease of use of the new system.*

Hypothesis 6 *Inertia will negatively impact perceptions of the relative advantage of the new system.*

Another possible effect is the direct negative influence of inertia on intention to use the new system [60]. This is beyond the impact mediated by beliefs. Previous research has shown that inertia can result in lowered usage intentions, despite knowledge that current practice is not the best [46]. In this regard, users may continue using manual password routines,

despite knowing that a personal password manager would be a better tool to manage account credentials. Thus, we propose:

Hypothesis 7 *Inertia will negatively impact intentions to use the new system.*

Lastly, there is evidence that inertia moderates the relationship between subjective norm and intention to use a new system. Analysis indicates that "*when an individual's inertia is high, social pressures to use a new system play a more important role in determining whether they will voice intentions to use the system*" [60]. Thus, social pressure is an important mechanism for change when high inertia is present. Because inert users lack motivation to fully assess alternatives, pressure from influential individuals in their social environment may shape their intention toward using the new system. The status quo bias perspective also posits that "*individuals often find that the path of least resistance is to conform to the institutional status quo*" [69]. Thus, if using a personal password manager is the social norm it will be more likely for users to switch to the new system. Thus, we propose:

Hypothesis 8 *Inertia will moderate the relationship between subjective norm and intentions to use the new system such that the relationship is stronger in the presence of high inertia.*

4 Validating the Model

A survey questionnaire is proposed to validate the model. A random sample of web users will be targeted using an online crowdsourcing platform (MTurk, Prolific.ac, or similar) with the requirement that participants should not currently be using a personal password manager.

The first part of the questionnaire will capture demographic information as well as current password practices. In this part we measure the participants' perception of confidence and pride with their current password routine (i.e. IKEA effect). We also include questions to assess perceived risk to their passwords.

The next part of the questionnaire prompts the user to investigate a personal password manager, as an alternative to their existing routine. LastPass was chosen as it is a well-known password manager with cross-platform and multi-device support. The user prompt is illustrated in Figure 4. Once participants return to the survey, they will be presented with three 'knowledge' test questions to confirm that they have examined the information about LastPass and understand its benefits.

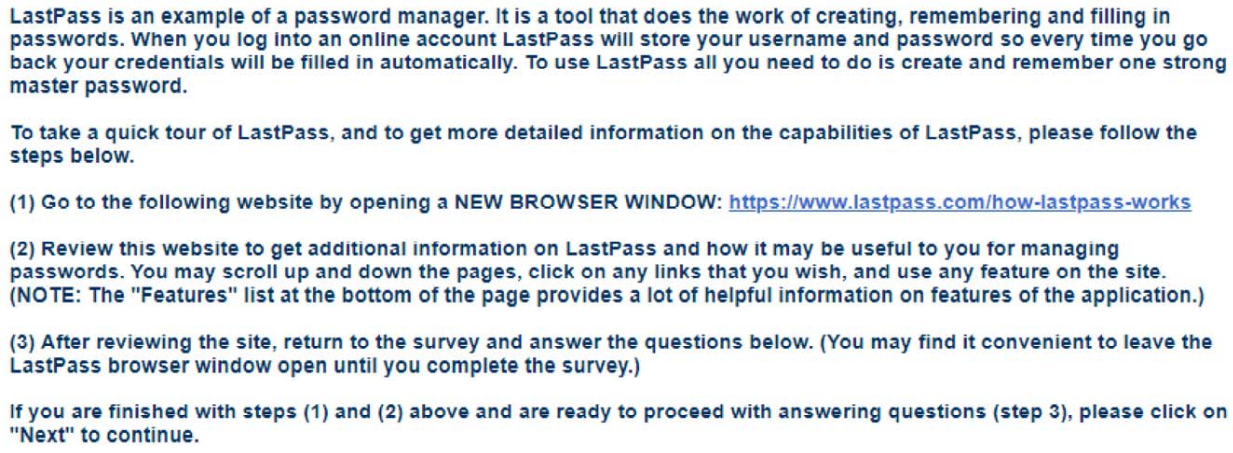

Figure 4: Introduction to LastPass

The final part of the questionnaire measures the remaining constructs of the model. Questions regarding the new system refer to LastPass, to make the notion of a personal password manager more concrete. Based on Polites and Karahanna [60], we used several existing and self-developed scales to measure the model constructs. Table 1 shows the construct source and item wording for each measure.

Table 1: Model Constructs and Measures

Transition Costs [53]	TC1	Learning how to use LastPass to manage my passwords would not take much time.
	TC2	Becoming skillful at using LastPass to manage my passwords would be easy for me.
Sunk Costs [53]		I have already invested a lot of time in...
	SC1	...learning to use my current routine to manage my passwords.
	SC2	...perfecting my skills at using my current routine to manage my passwords.
IKEA Effect (new, derived from [58, 52])	IE1	I have put a great deal of effort into coming up with my personal routine.
	IE2	I am proud of the way that I manage my passwords.
	IE3	Many people struggle to manage their passwords. I came up with a good solution.
	IE4	When I think about my password routine I feel proud.
	IE5	I describe my password routine to other people (without telling them enough to guess my passwords).
Inertia – Affective Based [60]		I [will] continue using my existing routine to manage my passwords...
	ABI1	... because it would be stressful to change.
	ABI2	... because I am comfortable doing so.
	ABI3	... because I enjoy doing so.
Inertia – Behavioral Based [60]		I [will] continue using my existing routine to manage my passwords...
	BBI1	... simply because it is what I have always done.
	BBI2	... simply because it is part of my normal routine.
	BBI3	... simply because I've done so regularly in the past.
Inertia – Cognitive Based [60]		I [will] continue using my existing routine to manage my passwords...
	CBI1	... even though I know it is not the best way of doing things.
	CBI2	... even though I know it is not the most efficient way of doing things.
	CBI3	... even though I know it is not the most effective way to do things.
Perceived Ease of Use [37, 79]	PEOU1	I would find LastPass easy to use for managing my passwords.
	PEOU2	Using LastPass to manage my passwords would be clear and understandable.
Relative Advantage [37, 79]		Using LastPass to manage my passwords, rather than my current routine to manage my passwords, would...
	RA1	...enhance my effectiveness.
	RA2	...increase my productivity.
	RA3	...improve my performance.
Subjective Norm (formative) [79]	SN1	People who influence my behavior think that I should use LastPass to manage my passwords.
	SN2	People who are important to me think that I should use LastPass to manage my passwords.
Internal Self-Efficacy [73]		I could use LastPass to manage my passwords if...
	SE1	...there was no one around to tell me what to do.
	SE2	...I had never used a system like it before.
	SE3	...I had only the online help for reference.
New System Usage Intention [79]	INT1	I intend to use LastPass to create and remember my passwords in the future.
	INT2	I plan to use LastPass to manage my passwords in the future.

5 Conclusion

People, even those with the requisite cybersecurity knowledge, often choose not to behave securely. They choose to stay with their familiar ways of doing things. This inertia is a form of resistance, and we need to understand the antecedents of inertia if we are to make a difference in this field.

We model password manager adoption because passwords, despite reports of their demise, continue to be the most popular authentication mechanism. Many organisations are implementing two factor authentication using applications such as Duo, but this does not remove the need for people to remember their primary password. We have proposed a model that models the impact of effort on inertia, and the impact of inertia on various constructs that prevent adoption.

The goal of this paper is to elicit workshop discussion on the applicability of resistance, and particularly inertia, in behavioural information security research. Inertia is an under-researched concept in information systems and, from our review of literature, also in the information security domain. We welcome input on the proposed model and our focus on *effort* and inertia as constructs that could be investigated in the behavioural information security field.

References

[1] I. Ajzen. The theory of planned behavior. *Organizational Behavior and Human Decision Processes*, 50(2):179–211, 1991.

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

[3] N. Alkaldi and K. Renaud. Why do people adopt, or reject, smartphone password managers? In *Proceedings European Workshop on Usable Security (EUROUsec)*, Darmstadt, Germany, 2016.

[4] N. Alkaldi and K. Renaud. Encouraging Password Manager Adoption by Meeting Adopter Self-Determination Needs. In *Proceedings of the 52nd Hawai'i International Conference on System Sciences*, Maui, Hawaii, January 2019.

[5] C. Alós-Ferrer, S. Hügelschäfer, and J. Li. Inertia and decision making. *Frontiers in Psychology*, 7:169, 2016. `https://doi.org/10.3389/fpsyg.2016.00169`.

[6] F. Alotaibi, S. Furnell, I. Stengel, and M. Papadaki. A review of using gaming technology for cyber-security awareness. *Int. J. Inf. Secur. Res.(IJISR)*, 6(2):660–666, 2016.

[7] A. Bandura. Social cognitive theory: An agentic perspective. *Annual Review of Psychology*, 52(1):1–26, 2001.

[8] A. Bandura and R. H. Walters. *Social learning theory*, volume 1. Prentice-hall, Englewood Cliffs, NJ, 1977.

[9] 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.

[10] A. Beaudry and A. Pinsonneault. The other side of acceptance: studying the direct and indirect effects of emotions on information technology use. *MIS Quarterly*, 34(4):689–710, 2010.

[11] 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, Lake Tahoe, CA, 2009. ACM.

[12] S. R. Boss, D. F. Galletta, P. Benjamin 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*, 39(4):837–864, Dec. 2015.

[13] J. C. Bruckman. Overcoming resistance to change: Causal factors, interventions, and critical values. *The Psychologist-Manager Journal*, 11(2):211–219, 2008.

[14] C.-Y. Chang and Y.-H. W. Taipei. An exploratory study on students' problem-solving ability in earth science. *International Journal of Science Education*, 24(5):441–451, 2002.

[15] J. C. Chang. An exploratory study on change resistance measurement. In *First International Technology Management Conference*, pages 885–891. IEEE, 2011.

[16] S. Chiasson and P. C. Van Oorschot. Quantifying the security advantage of password expiration policies. *Designs, Codes and Cryptography*, 77(2-3):401–408, 2015.

[17] M. C. Claudy, R. Garcia, and A. O'Driscoll. Consumer resistance to innovation—a behavioral reasoning perspective. *Journal of the Academy of Marketing Science*, 43(4):528–544, 2015.

[18] CompTIA Properties, LLC. Cybersecurity for Everyone, Not Just the IT Department, 2015. `https://cybersecure.org/pages/resources/CompTIA-CyberSecure-Human-Error-White-paper.pdf`.

[19] F. D. Davis. *A technology acceptance model for empirically testing new end-user information systems: Theory and results*. PhD thesis, Sloan School of Management, Massachusetts Institute of Technology, 1985.

[20] F. D. Davis. Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology. *MIS Quarterly*, 13(3):319–340, 1989.

[21] M. Donald. Organisational change factors: more than disgruntled employees or poor process. In *Proceedings of the Inaugural Australian Institute of Project Management 2016 National Conference, Hilton, Sydney, 16-19 October 2016*, pages 87–100, 2016.

[22] 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.

[23] L. S. Eckhardt, A. and T. Weitzel. Who influences whom? analyzing workplace referents' social influence on it adoption and non-adoption. *Journal of Information Technology*, 24(1):11–24, 2009.

[24] M. Fagan and M. M. H. Khan. Why Do They Do What They Do?: A Study of What Motivates Users to (Not) Follow Computer Security Advice. In *Twelfth Symposium on Usable Privacy and Security (SOUPS)*, pages 59–75, Denver, CO, 2016.

[25] D. Florencio and C. Herley. A Large-scale Study of Web Password Habits. In *Proceedings of the 16th International Conference on World Wide Web Banff, Alberta, Canada*, WWW '07, pages 657–666, New York, NY, USA, 2007. ACM.

[26] R. Folger and D. P. Skarlicki. Unfairness and resistance to change: Hardship as mistreatment. *Journal of Organizational Change Management*, 12(1):35–50, 1999.

[27] C. T. Fosnot and R. S. Perry. Constructivism: A psychological theory of learning. *Constructivism: Theory, Perspectives, and Practice*, 2:8–33, 1996.

[28] P. Gasti and K. B. Rasmussen. On the Security of Password Manager Database Formats. In S. Foresti, M. Yung, and F. Martinelli, editors, *European Symposium on Research in Computer Security (ESORICS)*, Lecture Notes in Computer Science, pages 770–787. Springer Berlin Heidelberg, 2012.

[29] J. L. Hale, B. J. Householder, and K. L. Greene. The theory of reasoned action. *The Persuasion Handbook: Developments in Theory and Practice*, 14:259–286, 2002.

[30] C. Herley and P. V. Oorschot. A Research Agenda Acknowledging the Persistence of Passwords. *IEEE Security & Privacy*, 10(1):28–36, Jan. 2012.

[31] P. Hsieh and W. Lin. Explaining resistance to system usage in the pharmacloud: A view of the dual-factor model. *Information & Management*, 55(1):51–63, 2018.

[32] N. Humaidi and V. Balakrishnan. Exploratory factor analysis of user's compliance behaviour towards health information system's security. *Journal of Health & Medical Informatics*, 4(2):2–9, 2013.

[33] M. Inzlicht, A. Shenhav, and C. Y. Olivola. The Effort Paradox: Effort Is Both Costly and Valued. *Trends in Cognitive Sciences*, 22(4):337–349, Apr. 2018.

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

[35] J. T. Jost. Resistance to change: A social psychological perspective. *Social Research: An International Quarterly*, 82(3):607–636, 2015.

[36] 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.

[37] E. Karahanna, R. Agarwal, and C. M. Angst. Reconceptualizing compatibility beliefs in technology acceptance research. *MIS Quarterly*, pages 781–804, 2006.

[38] K. Kato and V. Klyuev. Strong passwords: Practical issues. In *2013 IEEE 7th International Conference on Intelligent Data Acquisition and Advanced Computing Systems (IDAACS)*, volume 02, pages 608–613, Sept. 2013.

[39] H.-W. Kim. The effects of switching costs on user resistance to enterprise systems implementation. *IEEE Transactions on Engineering Management*, 58(3):471–482, 2010.

[40] 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.

[41] 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.

[42] E. S. Knowles and J. A. Linn. The importance of resistance to persuasion. In E. S. Knowles and J. A. Linn, editors, *Resistance and Persuasion*, chapter 1. Lawrence Erlbaum, 2003.

[43] K. Korpela. Improving cyber security awareness and training programs with data analytics. *Information Security Journal: A Global Perspective*, 24(1-3):72–77, 2015.

[44] 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.

[45] B. Lebek, J. Uffen, M. Neumann, B. Hohler, and M. H. Breitner. Information security awareness and behavior: a theory-based literature review. *Management Research Review*, 37(12):1049–1092, 2014.

[46] D. Lending and D. W. Straub. Impacts of an Integrated Information Center on faculty end-users: A qualitative assessment. *Journal of the American Society for Information Science*, 48(5):466–471, 1997.

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

[48] Z. Li, W. He, D. Akhawe, and D. Song. The Emperor's New Password Manager: Security Analysis of Web-based Password Managers. In *23rd USENIX Security Symposium*, pages 465–479, 2014.

[49] C. Luevanos, J. Elizarraras, K. Hirschi, and J. Yeh. Analysis on the Security and Use of Password Managers. In *2017 18th International Conference on Parallel and Distributed Computing, Applications and Technologies (PDCAT)*, pages 17–24, Dec. 2017.

[50] R. Maclean and J. Ophoff. Determining key factors that lead to the adoption of password managers. In *International Conference on Intelligent and Innovative Computing Applications (ICONIC)*, pages 1–7. IEEE, 2018.

[51] 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.

[52] 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, Dec. 2012.

[53] J. B. Moore. *Information Technology Infusion: A Motivation Approach*. PhD thesis, Florida State University, Tallahassee, 2000. Unpublished PhD Thesis.

[54] F. Mwagwabi, T. McGill, and M. Dixon. Improving Compliance with Password Guidelines: How User Perceptions of Passwords and Security Threats Affect Compliance with Guidelines. In *47th Hawaii International Conference on System Sciences*, pages 3188–3197, Jan. 2014.

[55] D. S. Nagin and G. Pogarsky. Integrating celerity, impulsivity, and extralegal sanction threats into a model of general deterrence: Theory and evidence. *Criminology*, 39(4):865–892, 2001.

[56] R. S. Nickerson. Confirmation bias: A ubiquitous phenomenon in many guises. *Review of General Psychology*, 2(2):175–220, 1998.

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

[58] 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.

[59] 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.

[60] 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), 2012.

[61] C. Posey, T. L. Roberts, P. B. Lowry, and R. T. Hightower. Bridging the divide: A qualitative comparison of information security thought patterns between information security professionals and ordinary organizational insiders. *Information & Management*, 51(5):551–567, 2014.

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

[63] K. Renaud. Blaming noncompliance is too convenient: What really causes information breaches? *IEEE Security & Privacy*, 10(3):57–63, 2011.

[64] K. Renaud, R. Otondo, and M. 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*, 82:241–260, 2019.

[65] K. Renaud, M. Volkamer, and A. Renkema-Padmos. Why doesn't Jane protect her privacy? In *International Symposium on Privacy Enhancing Technologies Symposium*, pages 244–262. Springer, 2014.

[66] K. Renaud and V. Zimmermann. Encouraging password manager use. *Network Security*, June:20, 2019.

[67] E. M. Rogers. *Diffusion of Innovations*. Free Press, New York, 4 edition, 1995.

[68] R. W. Rogers. A protection motivation theory of fear appeals and attitude change. *The Journal of Psychology*, 91(1):93–114, 1975.

[69] W. Samuelson and R. Zeckhauser. Status quo bias in decision making. *Journal of Risk and Uncertainty*, 1(1):7–59, 1988.

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

[71] R. Smollan. Engaging with resistance to change. *University of Auckland Business Review*, 13(1):12, 2011.

[72] 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.

[73] J. B. Thatcher, J. C. Zimmer, M. J. Gundlach, and D. H. McKnight. Internal and external dimensions of computer self-efficacy: An empirical examination. *IEEE Transactions on Engineering Management*, 55(4):628–644, 2008.

[74] K. Thomson and J. Van Niekerk. Combating information security apathy by encouraging prosocial organisational behaviour. *Information Management & Computer Security*, 20(1):39–46, 2012.

[75] B. Ur, P. G. Kelley, S. Komanduri, J. Lee, M. Maass, M. L. Mazurek, T. Passaro, R. Shay, T. Vidas, L. Bauer, N. Christin, and L. F. Cranor. How Does Your Password Measure Up? The Effect of Strength Meters on Password Creation. In *Proceedings of the 21st USENIX Conference on Security Symposium*, Security'12, Berkeley, CA, USA, 2012. USENIX Association.

[76] S. Van Acker, D. Hausknecht, W. Joosen, and A. Sabelfeld. Password Meters and Generators on the Web: From Large-Scale Empirical Study to Getting It Right. In *Proceedings of the 5th ACM Conference on Data and Application Security and Privacy*, CODASPY '15, pages 253–262, San Antonio, Texas, USA, 2015. ACM.

[77] 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.

[78] A. Vance, D. Eargle, K. Ouimet, and D. Straub. Enhancing Password Security through Interactive Fear Appeals: A Web-Based Field Experiment. In *2013 46th Hawaii International Conference on System Sciences*, pages 2988–2997, Jan. 2013.

[79] V. Venkatesh, M. G. Morris, G. B. Davis, and F. D. Davis. User acceptance of information technology: Toward a unified view. *MIS Quarterly*, pages 425–478, 2003.

[80] 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.

[81] R. Wash, E. Rader, R. Berman, and Z. Wellmer. Understanding Password Choices: How Frequently Entered Passwords Are Re-used across Websites. In *Twelfth Symposium on Usable Privacy and Security (SOUPS)*, pages 175–188, Denver, CO, 2016.

[82] D. T. Wegener, R. E. Petty, N. D. Smoak, and L. R. Multiple routes to resisting attitude change. In E. S. Knowles and J. A. Linn, editors, *Resistance and Persuasion*, chapter 3. Lawrence Erlbaum, 2003.

[83] 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.

[84] Z. Yunos, R. S. Ab Hamid, and M. Ahmad. Development of a cyber security awareness strategy using focus group discussion. In *SAI Computing Conference*, pages 1063–1067. IEEE, 2016.

[85] B. Zandvoort. On Inertia: Resistance to Change in Individuals, Institutions and the Development of Knowledge. *Cosmos and History: The Journal of Natural and Social Philosophy*, 11(1):342–360, 2015.

[86] L. Zhang-Kennedy, S. Chiasson, and P. v. Oorschot. Revisiting password rules: facilitating human management of passwords. In *2016 APWG Symposium on Electronic Crime Research (eCrime)*, pages 1–10, June 2016.

[87] V. Zimmermann and K. Renaud. Moving from a "Human-as-Problem" to a "Human-as-Solution" Cybersecurity Mindset. *International Journal of Human Computer Studies*, 131:169–187, 2019. November 2019.