Journal of Applied Research in Memory and Cognition 9 (2020) 345–354

Contents lists available at ScienceDirect

Journal of Applied Research in Memory and Cognition

journal homepage: www.elsevier.com/locate/jarmac

Surviving in the Digital Environment: Does Survival Processing Provide an Additional Memory Benefit to Password Generation Strategies?

Isis Chong, Robert W. Proctor*, Ninghui Li and Jeremiah Blocki

Purdue University, USA

People encouraged to think about their survival when encoding information experience a memory advantage even when compared to other tried-and-true methods. Despite the evidence in support of the survival-processing advantage, how this advantage might apply to current-day issues has received little attention. This study aimed to determine if password generation strategies modified to encourage fitness-related encoding would yield an additional benefit in password recall. Participants recruited from online and college samples generated passwords using a sentence-based mnemonic (pilot experiment and Experiment 1) or person-action-object strategy (Experiments 2 and 3), in survival or control scenarios. Results support the plausibility of implementing different strategies for password generation, particularly the person-action-object strategy, and the importance of providing users instructions with which to create their passwords. Although the results illustrated the value of using scenarios for password creation, they did not show evidence of an additional fitness-related benefit, for possible reasons that we discuss.

General Audience Summary

Users often have difficulty creating complex passwords that they can remember. This issue is exacerbated by the many online accounts that users must manage on any given day. The primary focus of the present study was to investigate password generation strategies that would help everyday users manage their passwords better. The study aimed to introduce into the cyber domain work from memory research that has shown human memory to be aided when information is processed in relation to one's survival. Two password generation strategies were examined that have been shown to be effective for memorability and security: one based on developing a sentence mnemonic and another related to stringing together pre-selected words (i.e., person-action-object strategy). Passwords generated using these strategies were created with either a survival scenario (e.g., surviving in a foreign land) or non-survival scenario (e.g., vacationing in a foreign land) in mind. Further, this study investigated password behaviors in two distinct user groups—those recruited from an online crowdsourcing pool and those recruited from a university participant pool. Password recall was examined over a one-week period. The results support the plausibility of implementing the person-action-object strategy as recall remained high even after a delay. However, no additional benefit was found with that strategy or the sentence-based strategy for conditions involving survival processing. Future directions for testing conditions under which survival may be effective within the context of password generation are discussed.

Keywords: Cybersecurity, Password memorability, Password retention, Survival processing

Author Note

Isis Chong & Robert W. Proctor, Department of Psychological Sciences, Purdue University, USA.

Ninghui Li & Jeremiah Blocki, Department of Computer Science, Purdue University, USA.

* Correspondence concerning this article should be addressed to Robert W. Proctor, Department of Psychological Sciences, Purdue University, West Lafayette, IN 47907, USA. Contact: rproctor@purdue.edu

Passwords are a ubiquitous part of modern life. To provide effective security, they must be character strings that are difficult for hackers to crack. However, because secure passwords are rarely memorable, users typically sacrifice security for memorability (Vu et al., 2007; Yan, Blackwell, Anderson, & Grant, 2004). Although some suggest that passwords are an outdated form of authentication that will be replaced (e.g., Bonneau, Herley, van Oorschot, & Stajano, 2012), users likely will have to continue to create and manage multiple passwords in the foreseeable future. Consequently, a goal is to develop methods to improve the memorability and security of user-generated passwords (Adams & Sasse, 1999; Chong, Xiong, & Proctor, 2019).

Most websites require that passwords contain letters, special characters, and digits. Many users satisfy this requirement by selecting a word and modifying it. The word "donkey," for instance, could be transformed into the password "d0nk3y!". However, because people construct their passwords systematically (Komanduri et al., 2011), hackers can predict how passwords are modified. Thus, other strategies have been created to help users move away from more stereotypical passwords.

One suggested password generation strategy is based on a memorized sentence. The first letters of each word are concatenated to make a password. Certain characters in the string may be modified to fit the requirements of a particular website. The generated passwords are less predictable than the aforementioned single-word strategy (Vu et al., 2007) and should be relatively memorable. A study comparing different sentence-based mnemonic password strategies revealed that the manner in which instructions are presented can significantly affect the security of the passwords. Yang, Li, Chowdhury, Xiong, and Proctor (2016) demonstrated that passwords generated to be personalized (e.g., "I went to London four and a half years ago") are more memorable than generic passwords (e.g., "Four score and seven years ago our fathers brought forth on this continent"). In general, the sentence-based mnemonic strategy has been shown to be useful for creating secure *and* memorable passwords.

Another promising strategy for password generation is that of person-action-object (PAO), which also yields passwords that are memorable and secure (Blocki, Komanduri, Cranor, & Datta, 2015). This strategy requires users to select a Person from a predetermined list, which a computer then pairs with an Action and an Object. Participants are to imagine this PAO string in different contexts. Although extensive research on various other methods of password recall and generation has been conducted, we restrict the present study to the sentence-based and PAO strategies, given their prior success.

Despite the large number of studies that have targeted password generation, few efforts have been made to tie the robust findings from laboratory memory experiments to cyber problems. The present study aims to bridge this gap by applying findings from adaptive memory research to password generation and retention.

In the last 15 years, researchers have argued that memory is adaptive and tuned to process survival-related information (Nairne, Thompson, & Pandeirada, 2007). Based on the notion that human memory evolved in a similar manner to bipedalism and other traits, Nairne et al. have posited that human memory is sensitive to information relevant to our fitness. They have provided evidence that processing information relative to one's survival can aid later recall, which is known as the survival-processing advantage. Since the initial demonstrations of the survival-processing advantage for recall and recognition, the notion that people benefit from processing information in regard to their survival has garnered significant support from other researchers (Kazanas & Altarriba, 2015). Findings have been replicated across many studies (e.g., Kang, McDermott, & Cohen, 2008; Weinstein, Bugg, & Roediger, 2008) and reproducibility efforts have supported the survival-processing advantage (Müller & Renkewitz, 2015).

Given the search for the effective password generation strategies and the possibility of extending the survival-processing advantage to these efforts, we attempted to determine the feasibility of taking what has been described as a stone-age adaptation (Nairne & Pandeirada, 2008) and applying it to cybersecurity. We conducted experiments designed to determine whether instructing participants to create passwords within survival-related scenarios affords a recall benefit beyond those already provided by the sentence-based mnemonic and PAO strategies. In a pilot experiment, described in the Supplemental Materials, participants recruited through online crowdsourcing (Amazon Mechanical Turk; MTurk) were tasked with using the sentence-based mnemonic strategy to generate a password that was meaningful to themselves (control) or meaningful for their survival (survival). Based on the results of this initial experiment, which provided no evidence of recall benefit for survival processing, we designed three experiments to address possible issues with the pilot study's design and to systematically evaluate survival-related scenarios in various contexts.

In Experiment 1, participants recruited from a university participant pool used the sentence-based mnemonic strategy but were instructed to think of an instance in which they experienced a threatening (survival) or pleasant (control) situation. In Experiment 2, university participants used the PAO strategy to create a password relevant to another person's vacation (control) or survival. Unlike the prior experiments, participants were only allowed to select from a list of predetermined words to create their passwords. In Experiment 3, participants were assigned a password string created using the PAO strategy and did not select the terms for the string. A control condition with no scenario was also included for comparison. In all experiments, the foremost concern was memorability of the generated passwords with the respective strategies and whether an emphasis on survival yielded a recall benefit beyond that of non-survival scenarios.

Experiment 1

Although the pilot experiment did not reveal differences in recall between survival and control conditions, a low return rate for the second session (29%) and the specific scenarios used may have contributed to the lack of effect. Consequently, we designed Experiment 1 to circumvent these possible problems by making three critical changes. To improve return rates, participants were recruited from a university participant pool instead

of MTurk, and they were told that the experiment was multi-session when they signed up and were reminded at the beginning and end of the first session that they were to return a week later. The third change was in wording of the encoding scenarios. In the pilot experiment, the instructions were to create a sentence that was meaningful to oneself or to one's survival, which may have been insufficiently specific for the encoding to be performed in the manner intended. Therefore, in Experiment 1 we instructed participants to imagine one particular instance in their lives in which they experienced a threatening or pleasant situation. Pleasantness conditions have been demonstrated to be effective at promoting recall (Nairne et al., 2007).

Method

Participants. Participants were 62 students from Introductory Psychology classes at Purdue University who received credit toward a research participation requirement. The majority of participants across experiments had self-reported average computer experience. A demographic information breakdown for all experiments can be found in the Supplementary Materials.

To take part, participants were required to sign up for both sessions, at the same time of day, a week apart. The sample size was determined based on past password studies using university students to test multiple passwords (e.g., Haque, Wright, & Scielzo, 2013; Wiedenbeck, Waters, Birget, Brodskiy, & Memon, 2005). Participants were aware of needing to return for a second session and returned at a scheduled time 7 days later.

Procedure. For both sessions, participants were seated in a testing room by themselves in front of a desktop computer and proceeded through the experiment at their own pace, as would be the case in a real-world scenario. They were tested in two experimental sessions that were one week apart. Participants were randomly assigned to one of the generation conditions in this experiment and in all the other experiments. During the first session, participants were introduced to the mnemonic generation method and were required to submit a sentence based on either the pleasantness or survival scenario, which they then concatenated into a password. All participants were instructed to imagine that they were creating a password for an account on a simulated site. Emphasis was placed on creating a new password that they had not previously used. These instructions were provided across all experiments in this study.

The generation phase was followed by a two-minute *Where's Waldo?* visual search distractor task. Participants were then tested on recall their passwords after the 2-min delay and, finally, participants completed a post-session questionnaire related to their demographics and likelihood to use the password strategy in the future. This post-session questionnaire was used throughout all of the experiments at the end of the first session. In this experiment and the others, participants were specifically instructed to abstain from writing down their passwords.

After the 7-day delay, participants returned to the lab to test again their recall of the password on the same simulated site and complete an additional demographics questionnaire. The second session included three phases: password recall, a demographic questionnaire, and an internet-related behaviors questionnaire. For password recall, no mention was made of recalling the sentence that was used. In both sessions, no time limits were placed on how much time participants had to generate the passwords or recall them at either time delay. Additionally, participants were given only one attempt to recall their passwords and were not provided feedback on their accuracy. In Experiment 1 and across all other experiments, participants were asked to report on the perceived accuracy of their recall during the second session and they were only given one opportunity to enter their password without feedback across sessions.

Mnemonic strategy. Participants were told to create a password based on a sentence relating to one of two scenarios. Instructions were modified so that password sentences were to be created based on a particular instance in the participant's life. The survival and pleasantness conditions asked participants to imagine a threatening or pleasant situation, respectively. The pleasantness condition was selected for comparison as it has been previously established to be an effective method of encoding (e.g., Nairne et al., 2007). The instructions were as follows with words differing between conditions presented in bold:

> Think of a memorable sentence or phrase related to a point in time in which you experienced a **pleasant/threatening** situation. This sentence should be meaningful to you and one that other people are unlikely to use. The sentence or phrase should contain at least eight words.
>
> Select a letter, number, or a special character to represent each word. A common method is to use the first letter of every word. Your password should be at least 8 characters long and should include at least one non-letter (e.g., 9; %).

The examples were generated by the experimenters and differed between the two conditions. The examples for the pleasantness condition were as follows: "Dinner three nights ago made me feel happy", dinner ⇒ d, nights ⇒ n, ago ⇒ @, password: dtn@mmfh; "I went on a nice hike in late 2016", went ⇒w, on ⇒ o, 2016 ⇒ 16, password: iwoanhil16.

The examples for the survival condition were as follows: "Dinner three nights ago made me feel sick", dinner ⇒ d, nights ⇒ n, ago ⇒ @, password: dtn@mmfs; "I went on a scary hike in late 2016", went ⇒w, on ⇒ o, 2016 ⇒ 16, password: iwoashil16.

Results

Passwords generated. Select examples of passwords that were created for the pleasantness and survival conditions can be found in Table 1. On average, passwords created for the pleasantness and survival conditions were 10 and 9 characters long, respectively. A total of 71% of passwords in the survival condition were identified as being strictly related to a threatening situation and without room for ambiguity. This count excluded passwords such as "I went to Ireland in 2018" and "yesterday I walk to the store with three people", as they were not entirely unambiguous.

Recall. Two chi-squared tests of independence were conducted to determine the relationships between recall after a

Table 1
Select Examples of Sentences and Passwords Created for the Survival and Pleasantness Conditions for Experiment 1

Survival	Pleasantness
My sister had a seizure when I was 6 (`mshaswiw6`)	Having my first kiss with chris november (`hmfkwc11`)
The earthquake in 2011 made me really scared (`Tei2mers`)	I went to seaside oregon in 2015 (`iwtsoi15`)
I fell up a goat path at Philmont (`ifâgpap`)	The Walk the Moon concert was the best (`twtmcwtb*`)

2-minute and 7-day delay and between the pleasant and survival conditions. The return rate after a 7-day delay was 87% for both conditions ($n_{pleasant} = 27$; $n_{survival} = 27$).

The relationship between recall and encoding condition shortly after password generation (i.e., after the 2-min delay) was not significant, $\chi^2(1, N = 62) = 2.95$, $p = .09$. Recall rates following the 2-minute delay were 84% and 97% for the pleasantness and survival conditions, respectively, consistent with a survival-processing benefit. However, the comparatively lower recall rate produced in the pleasantness condition at this short delay was due mostly to typos (e.g., "`iltpbkbed`" and "`iltpbkaed`"; "`3ya@siwh`" and "`tya@siwh`") in which the recalled password did not differ from the original password by more than one character.

Of more relevance to everyday password use, the relationship between recall and encoding condition after a 7-day delay also was not significant, $\chi^2(1, N = 54) = 1.95$, $p = .16$, with the tendency being opposite that of a survival-processing benefit: Recall rate was numerically lower for the survival condition (52%) than for the pleasantness condition (70%). Errors produced after a week were not as systematic as those found after a 2-min delay and typically involved several incorrect characters.

Subjective judgments. When asked about their likelihood to use the sentence-based mnemonic strategy they learned in the future during the first session, 28% of participants reported that they would be either "extremely likely" or "moderately likely" to use the strategy. Relative to the neutral value, the majority of responses were positive.

Discussion

Attrition was much lower in this experiment with the college students who were aware that they were to return for a second session than with the crowdsourcing participants in the pilot experiment who were unaware there would be a second session. Despite this difference and the changes in instructions, the results showed little evidence of a survival-processing benefit. At the 2-min delay the survival group had a numerically higher recall rate, but examination of the errors suggests that this difference was due mainly to an ancillary factor (typographical errors) rather than survival processing per se. At the 7-day delay, the nonsignificant numerical difference in recall was counter to the survival processing hypothesis. The overall recall rate of 60% at the 7-day delay was considerably higher than that of 22% in the pilot experiment, yet no survival-processing benefit was apparent in either case.

Experiment 2

The research conducted on the survival-processing advantage has predominantly used word lists as stimuli (e.g., Nairne et al., 2007). These lists are typically created by the experimenters from word norms and do not involve content that is self-generated by the participants, as in the pilot experiment and Experiment 1. Provision of the to-be-remembered words is not customary with password generation in everyday life.

However, work by cybersecurity researchers has suggested that selecting terms from preexisting lists may be an effective method for generating passwords. In Blocki et al.'s (2015) PAO strategy, users select a Person from a predetermined list. They then imagine a PAO scenario with Action and Object terms provided. For instance, participants may imagine Darth Vader (person) bribing (action) a roach (object) among lily pads. Recalling the scenario can aid later attempts to recall the password string ("darthvaderbribingroach"). Blocki et al. reported that this method circumvents much of the forgetting that tends to happen soon after password encoding. The story-based nature of the PAO strategy and the use of experimenter-generated word lists renders the strategy more similar to the typical study that shows a survival-processing advantage. Consequently, we turned to a survival-based PAO strategy to evaluate whether a survival scenario provides a recall benefit over other scenarios.

Method

Participants. A new set of 68 students who had not previously participated in this study were recruited from Purdue University and received course credit for their participation. Participants were scheduled to take part in the second session 7 days after the first session.

Person-Action-Object strategy. The PAO method used in the present study was based on the methodology used by Blocki et al. (2015) but differed along two critical dimensions. First, participants were allowed to select all three items to be used for the PAO string. Although Blocki and colleagues allowed users to select only the Person for the PAO string while a computer selected the corresponding Action and Object, this procedure was foregone to mirror more closely the protocols used with traditional word lists. The lists used in the original study were extensive and as such were abbreviated to facilitate the participant's search when presented in a dropdown list. The complete list of Person, Action, and Object items used in this study can be found in the Appendix. Second, Blocki et al. were focused on assessing the long-term benefits of using the PAO strategy and tested participants past the 100-day mark. Although they were able to find a benefit for this strategy even after such an extensive

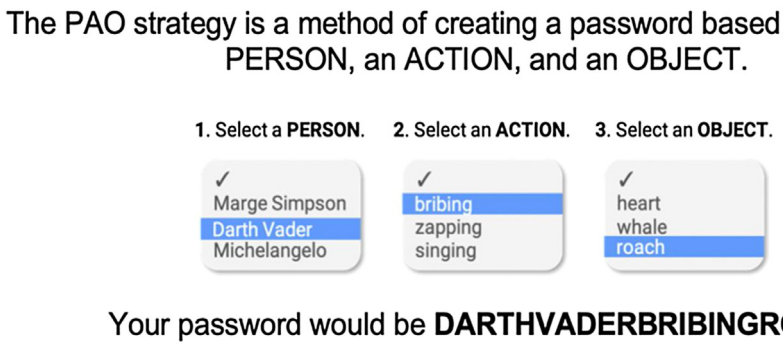

Figure 1. PAO generation instructions for both conditions.

delay, Experiment 3 was instead focused on the feasibility of incorporating survival-related processing into the PAO strategy. Consequently, long-term recall was measured only after a week.

To introduce the PAO strategy, participants were then given instructions and an example of how to use the strategy (Figure 1). The example featured short PAO lists that did not include terms that were included later in the experiment. The scenario instructions were as follows with words differing between conditions in bold:

> For this study you will be creating a PAO password based around **vacationing/surviving** in a foreign land. For instance, if your PERSON was **going to/strandedin** the grasslands of a foreign land, what ACTION could they take using an OBJECT to help ensure a **successful vacation/their survival**?

Procedure. Participants were seated in front of a desktop computer and proceeded through the experiment at their own pace. Participants were first given instructions on how to use the PAO method and then randomly assigned to one of two password generation conditions (i.e., vacation or survival). The generation condition to which participants were assigned determined the context for the selected PAO combination. Depending on the context, participants were to imagine their selected person acting upon an item to ensure a successful vacation or their survival in a foreign land. The participants were to enter the password they generated into a simulated shopping website. There were no time restrictions on how long participants had to create the password.

After the password generation phase, participants completed a two-min *Where's Waldo?* visual search distractor task. Following that task, participants were to recall their password once more on the simulated website with which they had been presented earlier. Finally, participants provided rationale for the PAO string they selected and completed a demographic questionnaire. Protocol for the second session after a 7-day delay was identical to that used in Experiment 2.

Results

Password generation. The PAO items selected from the predetermined wordlists had notable overlap. The most popular Person terms selected were Beyoncé (16%), Michael Phelps (9%), and Jay-Z (7%). The most popular Action terms selected were cooking (13%), swimming (13%), and flying (12%). The most popular Object term was "shark" (9%) with the rest of the Object terms being evenly distributed. There were two instances in which participants created the same password from the PAO list (i.e., "MichaelPhelpsswimmingshark"). Examples of PAO strings generated in the two conditions and the rationale provided by participants can be found in Table 2.

Recall. Two chi-squared tests of independence were conducted to determine the relationships between recall after 2-min and 7-day delays and between the vacation and survival conditions. The return rate after a 7-day delay was 97% for both conditions ($n_{vacation} = 34$; $n_{survival} = 32$).

The relationship between recall and encoding condition shortly after the 2-min delay was not significant, $\chi^2(1, N = 68) = 1.40$, $p = .24$. Recall rates for the control and survival conditions after a 2-min delay were 97% and 100%, respectively. Furthermore, following the 7-day delay, recall rates were 71% and 72% for the vacation and survival conditions, respectively. The relationship between recall and encoding condition after a 7-day delay also was not significant, $\chi^2(1, N = 66) = 0.01$, $p = .91$.

The errors committed following a one-week delay were found to be systematic and comparable across the two scenario conditions. We grouped them into six categories (Table 3). The largest number of errors ($n_{survival} = 2$; $n_{vacation} = 3$) involved misremembering the type of object (e.g., "cows" instead of "cow"). The next most common types of error involved the action term. These errors included misremembering the tense of the action term ($n_{survival} = 2$; $n_{vacation} = 2$; e.g., "cooks" instead of "cooking") or the type of action ($n_{survival} = 1$; $n_{vacation} = 2$; e.g., "moving" instead of "riding"). The remaining errors involved elaborating the original password to make a sentence with the three terms ($n_{survival} = 1$; $n_{vacation} = 1$), misremembering the person term ($n_{vacation} = 1$; i.e., "fode" instead of "Frodo") or making some other error unrelated to the term, such as a capitalization inconsistency ($n_{survival} = 3$; $n_{vacation} = 1$; "BILLGATESSWIMMINGSHARK" instead of "BillGatesSwimmingSharks").

Subjective judgments. When asked about the likelihood that they would use the sentence-based mnemonic strategy of the first session in the future, 28% of participants reported that they would be either "extremely likely" or "moderately likely" to use the strategy in the future.

Participants' subjective judgments about their performance mirrored their actual performance after a 7-day delay. When

Table 2
Select Examples of Passwords Created for the Survival and Vacation Conditions in Experiment 2 and the Rationale Provided by Participants for Their PAO Selections

Condition	Password	Rationale
Survival	Barackobamacookingfish	Barack Obama is stranded on a desert island and can only find fish in the ocean to feed himself. He must cook it in order to survive.
	Beyonceburyingcake	Beyoncé kicking up her heels in her signature dance moves, burying a piece of cake as bait.
	TIGERWOODSHUNTINGSNAKE	I imagined Tiger Woods hunting a snake for survival.
Vacation	PopeFranciscookingcake	Pope Francis went on vacation in Italy and decided to cook Italian cream cake for dessert.
	Barackobamasippingcoffee	I imagined Barack Obama laying on the beach and drinking coffee.
	Jayzmovingjeep	I imagined Jay-Z driving a Jeep around.

asked to rate their accuracy in recalling their passwords after the 7-day delay, 76% of people reported their performance as "extremely accurate" ($n = 40$) or "moderately accurate" ($n = 12$). Of these 52 participants, 75% were able to recall their passwords correctly. Furthermore, 85% of people rated the ease of recalling their passwords as "extremely easy" ($n = 29$) or "moderately easy" ($n = 29$). Of these 58 participants, 74% were able to recall their password correctly.

Discussion

Experiment 2 provided support for the PAO strategy, a list-based password generation technique, but did not show any systematic difference between the vacation and survival-processing scenarios. Recall accuracy was high in both conditions, which may have introduced ceiling effects that prevented detection of condition differences. All participants remembered their passwords without any or only minor mistakes. The tendency to retain the gist of the password when using the PAO strategy is striking considering that password recall is typically quite low. Additionally, note that the recall rates obtained in this study were higher than those utilizing different strategies at similar delays (e.g., Haque, Al-Ameen, Wright, & Scielzo, 2017).

Experiment 3

Although recall can currently be compared across the groups as in the previous experiments, a more ideal comparison to determine if there are survival-processing benefits may be one in which the same password string is examined across participants. As such, Experiment 3 was conducted to examine recall for pre-assigned passwords as well as using MTurk to recruit a larger sample size. Moreover, we added a control condition for which no scenario was mentioned in the instructions to verify the benefit of the PAO strategy. Finally, recall at a 2-min delay was not implemented to remove the possibility that this retrieval practice may have contributed in part to the high recall observed in Experiment 2.

Method

Participants. A new set of 2279 participants were recruited through MTurk. The participants were compensated $0.50 for each session of the study with a maximum compensation of $1.00. Participants were excluded from the study if their Internet Protocol (IP) address was found to be duplicated in our records. This was done to ensure that MTurk workers only participated once in the first part as duplicate IP addresses might indicate that a participant had multiple MTurk accounts that were accessed from the same location. Participants were also excluded if they did not follow experiment instructions (e.g., entered two distinct passwords instead of one).

PAO strategy. Participants were randomly assigned to one of two PAO strings (i.e., BeyoncéCookingShark or Jay-ZSwimmingCake). These two strings were used based on the most popular items selected in Experiment 2. Participants were not given explicit instructions to type either celebrity name with either an accent or a hyphen, respectively, and the absence of either was not coded as an incorrect entry when entering their password string into the site for the first time. Participants were instructed to employ the PAO strategy with one of three types of instructions: (a) instructions not mentioning a scenario, (b) instructions directing them to use a survival scenario, or (c) instructions directing them to use a vacation scenario.

Table 3
Time 2 Incorrectly Recalled Password Exemplars and Counts for Experiment 2. Emphasis has been Added to Highlight Relevant Errors

Type of error	Password generated at Time 1	Password recalled at Time 2	Count
Object Type	lukeskywalkercookingcow	lukeskywalkercooking**cows**	5
Action Tense	PopeFranciscookingcake	PopeFrancis**cooks**cake	4
Action Type	Jayzridingjeep	jayz**moving**jeep	3
Elaboration	Beyonceswimmingphone	beyonce**is**swimming**with**a**phone****inhand**	2
Person Type	Frodofiringphone	**fode**firephone	1

The two lattermost scenarios were identical to those used in Experiment 2.

Procedure. Participants were tested across two experimental sessions that were at least one week apart. Participants were randomly assigned to one of three scenario instructions conditions and one of the two PAO strings. During the first session, participants were introduced to the PAO strategy. Unlike the previous experiments, there was only one instance of recall during the first session when creating the password using the preassigned PAO string and there was no 2-min recall test thereafter. At the end of the session participants were asked to complete a questionnaire related to their computer experience. The post-test questionnaire concerning their willingness to adopt the PAO strategy in the future now included possible methods through which this might be achieved (i.e., using a mobile app or web browser). In an attempt to encourage higher return rates for the second session, participants were given additional reminders about returning at the beginning and end of the session.

The second session was completed between 7 and 9 days after the first session. The second session was shorter than the first session. Participants were only given a single attempt to recall their password and were not provided with feedback during the second session. Following password recall, participants were prompted to report the three PAO items in separate text boxes.

Results

Data handling. Of all of the cases, 29% ($n = 662$) were removed if participants did not follow the instructions related to using one of the two preselected passwords. The password strings that were entered by participants during the first session needed to include all three of the PAO terms with allowances for capitalization differences. Failure to include one or more of the components resulted in removal from the data set. Of the cases that were removed, 31% ($n = 206$) created their own PAO strings (e.g., `Keanufightingswords`). Although the goal of Experiment 3 was not to assess self-generated PAO passwords, these cases might be informative and, as such, are described at the end of the Results section. The final participant count for the first session was 1617.

Password string recall. The return rate after a 7- to 9-day delay was 44% for both conditions ($n_{control} = 260$; $n_{vacation} = 223$; $n_{survival} = 221$). Participants reported back, on average, on the 7th day ($SD = .5$). A chi-squared test of independence was conducted to determine the relationship between password recall and the three scenario instruction conditions (i.e., none, vacation, or survival). Password recall after a weeklong delay was compared to password entry during the first session. The relationship between recall and encoding condition shortly after password generation was significant, $\chi^2(2, N = 704) = 70.37$, $p < .001$. The correct recall rate for the condition without scenario instruction was 1.1%, whereas for the vacation and survival conditions, the recall rates were 27.8% and 20.8%, respectively. The greater recall for the scenario conditions than for the control condition indicates the well-established benefit of instructing participants to create an interactive mental image for verbal materials (Paivio, 1969). Although the recall rate was numerically higher for the vacation condition compared to the survival condition, the difference was not significant, $\chi^2(1, N = 444) = 2.95$, $p = .09$. Two additional chi-squared analyses for the scenario conditions did not reveal differences in recall between the Beyoncé or Jay-Z PAO strings for the survival, $\chi^2(1, N = 221) = .23$, $p = .63$, or vacation scenarios, $\chi^2(1, N = 223) = .73$, $p = .39$.

Recall of the PAO components. Average accuracy across the three separate PAO terms that were probed for at the end of the experiment was calculated across all participants. Accuracy scores for the three terms was either 0, 33, 67, or 100%. No differences in accuracy were found between the control ($M = 68\%$; $SE = 3\%$), vacation ($M = 68\%$; $SE = 3\%$), and survival conditions ($M = 64\%$; $SE = 3\%$), $F(2, 701) = .77$, $p = .46$. When average accuracy was restricted to participants who incorrectly recalled their exact password string, it was predictably lower and 57% for the two scenario conditions. The same breakdown based on accuracy for the no instruction condition was unchanged numerically (68%), but that is because almost all participants incorrectly recalled their password. These results suggest that the differences in recall for the exact password string between the conditions were not due to identifying the correct terms, but instead due to errors in recalling term order.

An additional ANOVA was run to determine if there were any differences in individual PAO term recall between the conditions for the two PAO strings. Similar to the primary analysis, no difference in accuracy wasfound ($F < 1.0$).

Subjective judgments. When asked about their likelihood to use the sentence-based mnemonic strategy if a mobile app or browser provided were to provide them with a list of pre-selected terms to generate a password using the PAO strategy, 39% of participants reported that they would be either "extremely likely" or "moderately likely" to use the strategy in the future.

Participants' subjective judgments about their performance reflected their actual performance after a 7-day delay more poorly than their counterparts in Experiment 3. When asked to rate their accuracy in recalling their passwords after the 7-day delay, 52% reported their performance as either "extremely accurate" ($n = 177$) or "moderately accurate" ($n = 191$). Of these participants, 27% were able to recall their passwords correctly. Additionally, 36% of people rated their ease of recalling their passwords as either "extremely easy" ($n = 91$) or "moderately easy" ($n = 162$). Of these participants, 26% were able to recall their password correctly.

Self-selected PAO strings. Of the 206 people who selected their own PAO strings, 40% ($n = 82$) returned a week later. Of these people, 13% ($n = 11$) were able to correctly recall their passwords. Of those who recalled their passwords, all but one had been given vacation or survival scenario instructions.

Discussion

When participants were not given scenario-related instructions in Experiment 3, recall for their password strings was much poorer than when instructions were given in Experiment 2. The near-ceiling results found in Experiment 2 when participants selected all of the terms that made up their PAO strings (after correcting for minor errors) were absent in Experiment 3 in which the terms were pre-selected. However, this comparison is only suggestive, given the other methodological differences between the experiments. Although exact recall of the passwords in Experiment 3 was imperfect, participants still recalled two of the three terms on average when tasked with reporting each PAO term. This result suggests that participants recalled the gist of their passwords. Participants' ability to recall a portion of the terms may have led to the over-reporting of subjective accuracy.

General Discussion

The study's results warrant discussion of three issues: support of the PAO strategy, the absence of an additional survival-processing benefit, and differences between crowdsourcing and university samples. First, how do the strategies employed in this study compare to other password studies independent of survival processing? Particular emphasis can be paid to the PAO strategy. When participants selected the terms for their PAO string (Experiment 2), recall was accurate, much more so than with the sentence-based mnemonic (pilot experiment and Experiment 1). Further, errors were systematic, and participants recalled the gist of their passwords. This is not surprising as the PAO sentences were considerably shorter, suggesting that strategies to be pursued should be relatively simple and straightforward.

The results also suggest that selecting one's own PAO terms may be critical in the memorability of the PAO strings. Recall was higher when the PAO terms were self-selected (Experiment 2) than when they were pre-selected (Experiment 3). However, the overlap in the selected terms may not be ideal for security as redundancy increases guessability. These results point to the possible importance of including users in the password generation process, though methodological differences (e.g., different participant pools; experimental settings) necessitate further investigation.

However, self-selection of PAO terms may result in a benefit to memorability at a cost to security. More secure passwords have greater randomness and are more difficult to guess. Computer-generated passwords are ideal for this purpose, as they can be chosen to avoid terms that would be commonly selected by users. The high-level retention observed with user-selected terms suggests that the most productive way forward may be to find some middle ground in which users select some terms while a computer selects others. Hypothetically, this could be implemented with a third-party application or browser extension.

Regarding the survival processing advantage, Nairne and Pandeirada (2016) stated, "The fact that survival processing may tap an evolved adaptation does not guarantee that it will produce a mnemonic benefit" (p. 502). Further, if encoding is constrained, the survival-processing benefit should be reduced or eliminated. As with other adaptations, boundary conditions do not negate the possibility of the evolutionary adaptation altogether. In our experiments, there was no evidence that incorporating survival processing into the password generation strategies provided an additional recall benefit compared to non-survival processing.

Traditionally, studies investigating the survival-processing advantage require that participants perform a surprise recall test after having encoded words they rated for relevance to survival and control scenarios (Nairne, Pandeirada, & Thompson, 2008). As participants rate words for relevance to a survival scenario and link them to it, they are not considering how and when they will recall these words. In all but the pilot experiment, participants were aware of the test that would occur later, and in all experiments, they were only responsible for a single password developed within the context of a sentence-based or PAO mnemonic strategy. It is plausible that the types of methods employed in our study are outside of the boundary conditions for the survival-processing advantage.

In what other cases has the survival-processing advantage been absent? Kroneisen and Erdfelder (2011) found that it vanished when the survival scenario was narrowed (i.e., focusing on finding potable water). Further, manipulating the word lists so that they were incongruent with a survival scenario erased the survival-processing advantage (Butler, Kang, & Roediger, 2009). In both cases, limiting the possible uses of an item reduced the ease with which it was recalled. These results suggest that elaboration is critical in the survival-processing advantage (Nairne & Pandeirada, 2016).

Similarly, the discrepancies between our results and those of previous studies may reside in the elaboration (or lack thereof) that was promoted. The methods we utilized to study a potential survival-processing benefit for passwords are distinct from the body of work that currently exists. It is possible that the lack of evidence of a survival-processing benefit in the present experiments was due to the depicted scenarios. Others investigating the survival-processing advantage have used long and detailed scenarios (e.g., Nairne et al., 2007). By comparison, our instructions were brief, which may have inadvertently discouraged elaboration. On the other hand, the password generation strategies themselves may have inherently created strong traces, which could not be further supplemented with a survival frame.

The findings highlight other key factors that were not the focus of the study. First, our use of crowdsourcing and university participant pools indicated differences between the groups. One of the most obvious was the participant return rate. Return rates for the university pool were over 80%, whereas those for the crowdsourcing sample ranged between 30% and 44%. Could these differences be related to motivation levels of the

two groups? Participants from the university pool are given the option of earning research credits through completing a library project. A majority of students choose to participate in research, but unexcused absences default them to the library project, so students try to attend all studies for which they sign up. The MTurk participants did not incur a similar penalty. Our results do not suggest any reason to suspect critical differences in results for the two participant pools, but this return-rate difference warrants future consideration (Haque et al., 2013).

Because this study is the first attempt to bridge work on survival processing and password generation, there is room for future development. In our experiments, participants created one password in isolation with no competing goals. The PAO strategy was effective at increasing password recall, but a survival scenario did not add further benefit. However, in everyday life, users typically create multiple passwords with more global goals in mind. Consequently, users may abandon elaborate strategies and revert to more straightforward password generation methods. Creating research environments that approximate such contexts should be informative as to whether the strategies are of value and a survival scenario beneficial when multiple passwords are required. Regardless, systematic consideration of human users is an essential part of the defense against adversary attacks.

Ethics Approval and Consent to Participate

All experiments were approved by the Purdue University Institutional Review Board (protocol # 1707019450). Participants consented to participate by clicking "next" at the bottom of a consent form page.

Availability of Data and Material

De-identified data can be made available upon reasonable request when the final manuscript is accepted for publication. Any data released will be managed to mitigate any privacy issues related to password release.

Conflict of Interest

None of the authors has a competing interest that conflicts with the study.

Funding

This research was supported by the National Science Foundation under Grant No. 1704587.

Author Contributions

All authors participated in conceiving and designing the experiments. I. Chong performed primary data collection, analysis, and interpretation, under the supervision of R.W. Proctor, N. Li, and J. Blocki. I. Chong drafted the manuscript, and she and R.W. Proctor jointly made the revisions. The other two authors provided feedback on the drafts of the manuscript. All authors approved the final version of the manuscript.

Appendix

Lists of Person, Action, and Object items adopted from Blocki et al. (2015).

People			
Ben Affleck	Pope Francis	Nelson Mandela	Justin Timberlake
Beyoncé	Frodo	Barack Obama	Kim Jong Un
Joe Biden	Gandalf	Rand Paul	Obi-Wan Kenobi
Kobe Bryant	Bill Gates	Ron Paul	Oprah Winfrey
George W. Bush	Adolf Hitler	Michael Phelps	Tiger Woods
Bill Clinton	Lebron James	Brad Pitt	Jay-Z
Hillary Clinton	Steve Jobs	Bart Simpson	Mark Zuckerberg
Albert Einstein	Angelina Jolie	Homer Simpson	
Jimmy Fallon	Michael Jordan	Luke Skywalker	

Actions			
bowing	fuming	moving	seizing
burying	giving	mopping	sheering
chipping	gluing	mowing	shining
choking	howling	nosing	signing
coating	hunting	oiling	sipping
combing	inhaling	paddling	stewing
concealing	judging	popping	stretching
cooking	juicing	pulling	sucking
copying	jumping	racing	swimming
drying	kissing	raking	taping
egging	knifing	reaching	tattooing
elbowing	muddying	riding	tazing
fanning	marrying	rolling	voting
firing	mauling	rowing	waking
flying	mashing	searing	waving

Objects			
apple	couch	lion	safe
arrow	cow	lock	sauce
beehive	daisy	mail	seal
bike	dove	menu	shark
boar	duck	moose	snake
bomb	fish	mummy	snow
bunny	goose	nail	soap
bus	hammer	owl	sumo
cab	hen	patty	teacup
cake	home	phone	tiger
canoe	hoof	pill	tire
chainsaw	jeep	puppy	toe
chili	jet	ram	vase
chime	kite	Rat	wagon
coffee	lime	Roach	wiener

Supplementary Data

Supplementary data associated with this article can be found, in the online version, at https://doi.org/10.1016/j.jarmac.2020.04.006.

References

Adams, A., & Sasse, M. A. (1999). Users are not the enemy: Why users compromise computer security mechanisms and how to take remedial measures. *Communications of the ACM*, *42*, 40–46. http://dx.doi.org/10.1145/322796.322806

Blocki, J., Komanduri, S., Cranor, L., & Datta, A. (2015). Spaced repetition and mnemonics enable recall of multiple strong passwords. In *22nd annual network and distributed system security symposium, NDSS 2015* http://dx.doi.org/10.14722/ndss.2015.23094

Bonneau, J., Herley, C., van Oorschot, P. C., & Stajano, F. (2012). The quest to replace passwords: A framework for comparative evaluation of web authentication schemes. In *Proceedings of the IEEE symposium on security and privacy* (pp. 553–567). http://dx.doi.org/10.1109/SP.2012.44

Butler, A. C., Kang, S. H., & Roediger, H. L., III. (2009). Congruity effects between materials and processing tasks in the survival processing paradigm. *Journal of Experimental Psychology: Learning, Memory, and Cognition*, *35*, 1477–1486. http://dx.doi.org/10.1037/a0017024

Chong, I., Xiong, A., & Proctor, R. W. (2019). Human factors in the privacy and security of the Internet of Things. *Ergonomics in Design*, *27*, 5–10. http://dx.doi.org/10.1177/1064804617750321

Haque, S. M. T., Al-Ameen, M. N., Wright, M., & Scielzo, S. (2017). Learning system-assigned passwords (up to 56 bits) in a single registration session with the methods of cognitive psychology. In *Proceedings of USEC'17* http://dx.doi.org/10.14722/usec.2017.23034

Haque, S. M. T., Wright, M., & Scielzo, S. (2013). A study of user password strategy for multiple accounts. In *Proceedings of the third ACM conference on data and application security and privacy* (pp. 173–176). http://dx.doi.org/10.1145/2435349.2435373

Kang, S. H., McDermott, K. B., & Cohen, S. M. (2008). The mnemonic advantage of processing fitness-relevant information. *Memory & Cognition*, *36*, 1151–1156. http://dx.doi.org/10.3758/MC.36.6.1151

Kazanas, S. A., & Altarriba, J. (2015). The survival advantage: Underlying mechanisms and extant limitations. *Evolutionary Psychology*, *13*, 360–396. http://dx.doi.org/10.1177/147470491501300204

Komanduri, S., Shay, R., Kelley, P. G., Mazurek, M. L., Bauer, L., Christin, N., ... & Egelman, S. (2011). Of passwords and people: Measuring the effect of password-composition policies. In *Proceedings of the SIGCHI conference on human factors in computing systems* (pp. 2595–2604). http://dx.doi.org/10.1145/1978942.1979321

Kroneisen, M., & Erdfelder, E. (2011). On the plasticity of the survival processing effect. *Journal of Experimental Psychology: Learning, Memory, and Cognition*, *37*, 1553–1562. http://dx.doi.org/10.1037/a0024493

Müller, S., & Renkewitz, F. (2015). Replication of study 2. In J. S. Nairne, J. N. S. Pandeirada, & S. Thompson (Eds.), *Open science framework: Reproducibility project* http://dx.doi.org/10.17605/OSF.IO/ZC468

Nairne, J. S., & Pandeirada, J. N. S. (2008). Adaptive memory: Remembering with a stone-age brain. *Current Directions in Psychological Science*, *17*, 239–243. http://dx.doi.org/10.1111/j.1467-8721.2008.00582.x

Nairne, J. S., & Pandeirada, J. N. S. (2016). Adaptive memory: The evolutionary significance of survival processing. *Perspectives on Psychological Science*, *11*, 496–511. http://dx.doi.org/10.1177/1745691616635613

Nairne, J. S., Pandeirada, J. N. S., & Thompson, S. R. (2008). Adaptive memory: The comparative value of survival processing. *Psychological Science*, *19*, 176–180. http://dx.doi.org/10.1111/j.1467-9280.2008.02064.x

Nairne, J. S., Thompson, S. R., & Pandeirada, J. N. S. (2007). Adaptive memory: Survival processing enhances retention. *Journal of Experimental Psychology: Learning Memory, and Cognition*, *33*, 263–273. http://dx.doi.org/10.1037/0278-7393.33.2.263

Paivio, A. (1969). Mental imagery in associative learning and memory. *Psychological Review*, *76*, 241. http://dx.doi.org/10.1037/h0027272

Vu, K. P. L., Proctor, R. W., Bhargav-Spantzel, A., Tai, B. L. B., Cook, J., & Schultz, E. E. (2007). Improving password security and memorability to protect personal and organizational information. *International Journal of Human-Computer Studies*, *65*, 744–757. http://dx.doi.org/10.1016/j.ijhcs.2007.03.007

Weinstein, Y., Bugg, J. M., & Roediger, H. L. (2008). Can the survival recall advantage be explained by basic memory processes? *Memory & Cognition*, *36*, 913–919. http://dx.doi.org/10.3758/MC.36.5.913

Wiedenbeck, S., Waters, J., Birget, J. C., Brodskiy, A., & Memon, N. (2005). PassPoints: Design and longitudinal evaluation of a graphical password system. *International Journal of Human-Computer Studies*, *63*, 102–127. http://dx.doi.org/10.1016/j.ijhcs.2005.04.010

Yan, J., Blackwell, A., Anderson, R., & Grant, A. (2004). Password memorability and security: Empirical results. *IEEE Security & Privacy*, *2*, 25–31. http://dx.doi.org/10.1109/MSP.2004.81

Yang, W., Li, N., Chowdhury, O., Xiong, A., & Proctor, R. W. (2016, October). An empirical study of mnemonic sentence-based password generation strategies. In *Proceedings of the 2016 ACM SIGSAC conference on computer and communications security* (pp. 1216–1229). http://dx.doi.org/10.1145/2976749.2978346

Received 9 February 2020;
received in revised form 15 April 2020;
accepted 18 April 2020
Available online 15 July 2020