2005

Visual recall cues for internet passwords

Mark Edward Wehner
San Jose State University

Follow this and additional works at: https://scholarworks.sjsu.edu/etd_theses

Recommended Citation

Wehner, Mark Edward, "Visual recall cues for internet passwords" (2005). *Master's Theses*. 2793.
DOI: <https://doi.org/10.31979/etd.gx5s-9ua2>
https://scholarworks.sjsu.edu/etd_theses/2793

This Thesis is brought to you for free and open access by the Master's Theses and Graduate Research at SJSU ScholarWorks. It has been accepted for inclusion in Master's Theses by an authorized administrator of SJSU ScholarWorks. For more information, please contact scholarworks@sjsu.edu.

VISUAL RECALL CUES FOR INTERNET PASSWORDS

A Thesis

Presented to

The Faculty of the Graduate Program in Human Factors / Ergonomics

San Jose State University

In Partial Fulfillment

of the Requirements for the Degree

Master of Science

By

Mark Edward Wehner

August 2005

UMI Number: 1429456

Copyright 2005 by
Wehner, Mark Edward

All rights reserved.

INFORMATION TO USERS

The quality of this reproduction is dependent upon the quality of the copy submitted. Broken or indistinct print, colored or poor quality illustrations and photographs, print bleed-through, substandard margins, and improper alignment can adversely affect reproduction.

In the unlikely event that the author did not send a complete manuscript and there are missing pages, these will be noted. Also, if unauthorized copyright material had to be removed, a note will indicate the deletion.

UMI[®]

UMI Microform 1429456

Copyright 2006 by ProQuest Information and Learning Company.

All rights reserved. This microform edition is protected against
unauthorized copying under Title 17, United States Code.

ProQuest Information and Learning Company
300 North Zeeb Road
P.O. Box 1346
Ann Arbor, MI 48106-1346

© 2005

Mark Edward Wehner

ALL RIGHTS RESERVED

APPROVED FOR THE PROGRAM OF
HUMAN FACTORS AND ERGONOMICS

Anthony D. Andre, Ph.D. Thesis Chair
Department of Industrial and Systems Engineering

Kevin M. Corker, Ph.D., Committee Member
Department of Industrial and Systems Engineering

John Boyd, Ph.D., Committee Member
Yahoo! Inc.

APPROVED FOR THE UNIVERSITY

08/31/05

ABSTRACT

VISUAL RECALL CUES FOR INTERNET PASSWORDS

by Mark E. Wehner

This thesis looked at aiding the recall of character-based passwords within internet authentication by placing retrieval cues in the login environment. This study investigated image cues, which were meaningful and represented real world objects, and pattern cues, which were abstract graphics with no meaning. Results showed that visual cue conditions did yield improved recall over having no cues. However there was no difference between image cues and pattern cues. Further qualitative results showed that participants did not find the cues helpful when recalling passwords as they could not make any associations between the cue and the password. We believe that within the context-dependent memory framework, the cues in this experiment were of incidental context rather than meaningful context. This suggests that although participants were not able to make associations between passwords and cues, the login page environment was a powerful catalyst for helping participants remember their passwords.

ACKNOWLEDGEMENTS

I would like to thank my thesis committee members John Boyd and Kevin Corker, and my thesis advisor Tony Andre. Their guidance and wisdom helped shape this project and made it a success.

I would also like to thank Jason Cara who built the experiment program that facilitated the experiment and collected the data. This project could not have been possible without his brilliance and generosity.

Finally, I would like to thank my friends and family for their moral support. I would especially like to thank JoAnne Deflino who provided the patience and support I needed to reach my goals.

TABLE OF CONTENTS

SECTION	PAGE
LIST OF TABLES.....	ix
LIST OF FIGURES.....	x
INTRODUCTION.....	1
Problem Statement.....	1
A Response to the Problem with Technology.....	3
Formal Observational Research on Users and Passwords.....	5
Human Memory: Why Do We Forget?.....	7
Experimental Research on Password Authentication.....	12
The Present Study.....	14
METHODS.....	16
Independent Variables.....	16
Dependent Measures.....	16
Participants.....	17
Visual Cue Stimuli.....	17
Login Name and Passwords.....	18
Procedure.....	18
Additional Experimental Controls.....	20
Hypothesis.....	21
RESULTS.....	22

SECTION	PAGE
Immediate Recall Test: Password Recall Success.....	23
Immediate Recall Test: Password Recall Time.....	28
One Week Recall Trials: Password Recall Success.....	33
One Week Recall Trials: Password Recall Time.....	35
Post Test Survey.....	38
DISCUSSION.....	46
Support for Recall Cues within the Login Environment.....	46
Incidental Contextual Cues.....	48
Cue Limitations: Long Term Effects.....	49
Consistency with Observational Research.....	50
Implications for Web Design.....	50
Limitations.....	51
Further Research.....	51
CONCLUSION.....	53
REFERENCES.....	55
Appendix A. Agreement to Participate in Research.....	60
Appendix B. Post-Test Survey.....	62
Appendix C. Task Protocol.....	64
Appendix D. Item Task Sheet.....	65
Appendix E. Passwords.....	66

SECTION	PAGE
Appendix F. Picture Cues.....	67
Appendix G. Login Screens Encountered by Participants.....	78
Appendix H. Independent and Dependent Variables.....	71

LIST OF TABLES

TABLE	PAGE
1. Immediate password recall success between all recall cues and the baseline.....	25
2. Immediate password recall success between conditions.....	26
3. Immediate password recall success between absent cues.....	27
4. Immediate password recall times between conditions for successful trials.	30
5. Immediate password recall times between conditions for failed trials.....	30
6. One week password recall partial success between conditions.....	34
7. One week password recall times.....	36
8. 1 week password recall times between cues and no cues.....	37

LIST OF FIGURES

FIGURE	PAGE
1. Immediate password recall success between all recall cues and the baseline.....	25
2. Immediate password recall success between conditions.....	26
3. Immediate password recall success between absent cues.....	27
4. Immediate recall time for both successful and failed trials between conditions.....	31
5. Interaction plot for immediate recall times.....	32
6. One week password recall partial success between conditions.....	34
7. One week password recall times between conditions.....	36
8. One week password recall times between cues and no cues.....	37
9. Matching success between web sites and recall cues.....	41
10. Matching Success between Image Cues and Pattern Cues.....	42
11. Frequency of sites requiring passwords.....	43
12. Unique passwords per site.....	44
13. Frequency of new account creation for forgotten passwords.....	44
14. Frequency of web site abandonment due to forgotten passwords.....	44
15. Frequency of changing passwords.....	45

INTRODUCTION

Problem Statement

With the rise of internet usage, we increasingly use online applications to manage our lives. People are going online to read newspapers, communicate with friends and family, manage their finances, shop using the vast number of e-commerce sites, and tap into various databases to retrieve such information as movie times and driving directions. However, to accomplish many of these tasks, users must authenticate themselves using character-based login names and passwords. Users must create and memorize passwords that are usually 5-6 characters long and many times have security restrictions. For example, a security restriction could be requiring the user to select one of the password characters a digit. Authentication is primarily used to give users entrance to exclusive online applications and content or for personalizing the online experience for the individual user. The main struggle regarding authentication is balancing the user's ability to remember meaningful passwords and security restrictions that often prevent users from creating easy to remember passwords.

In 1995 Jacob Nielsen proclaimed that, "user registration will have to die" because users will not be able to keep track of each individual password required for each website (Nielsen 1995). Nielson predicted that users would eventually have to write down their passwords or select easy to remember passwords, which would in turn jeopardize security. He remarked that users do not necessarily want to jeopardize their security, but there are only a few people in the world capable of remembering the 50 different secure random passwords for the 50 sites that the average person uses. Nielsen

further pointed out that forgotten passwords are the main cause for repeated registration and that users could have five to ten registered accounts within one website (Neilson 2000).

Similarly, a survey by Rainbow Technologies found that 55% of computer users have written down a password at least once and 40% have shared a password with someone else (Light 2003). They also found 90% of office workers at Waterloo Station in London gave away their computer password for a cheap pen. Further analysis showed that the most common passwords were the person's own name, favorite sports team, date of birth, and the word "password" itself.

The poor usability of authenticating users with passwords has always been a common complaint among HCI experts. Experts have pointed out that the numerous login names and passwords required by the average computer user causes many users to choose simple, and easy to remember passwords or develop the habit of writing down their passwords. However, it is behaviors like these that make it easier for hackers to gain access to accounts. What makes a password more memorable also makes it less secure Carroll (1996).

The conflict of ease-of-remembering vs. security has caused many usability experts to publish guidelines for creating "usable" security systems. Bruce Tognazzini (1999), for example, gave 12 guidelines stating that the main problem in this conflict is that security engineers have no training in Human Factors and end-up creating systems that are impossible for real people to use. These guidelines include allowing the user to

choose their own password and avoiding strange conditions such as making the first character a digit.

In 2003 the Communication Technologies Branch at the National Cancer Institute created web usability and design guidelines. Their site (www.usability.gov) points to “Reducing the user’s workload” as one of the most important and credible web guidelines and listed recalling passwords as one of the top tasks which taxes a user’s mental processing ability.

In summary, the usability of passwords has caused significant problems for users both in terms of memorization of passwords and in security. As the internet has led us to create more authentication passwords, the problem has become much more significant. In the next section this thesis will briefly describe how new technologies are being created to address the usability problem of passwords.

A Response to the Problem with Technology

Many companies have begun to create software programs to aid users to remember and use passwords. Software programs like AI Roboform, and Microsoft Windows password manager can store and automatically fill in the password for users when accessing websites. Similarly, many software programs have been created to store your login names and passwords. Since many users opt to write down their password anyway, software such as Passwords Plus help a user store and keep track of their login names and passwords rather than discourage such behaviors.

However, these methods are not without their own security flaws. For example, these methods do not protect you if someone accesses your computer, nor do they help a user who needs to access certain sites on a remote computer, which is the very convenience of web sites and web applications. Rainbow technologies has attempted to make the electronic storage of passwords mobile by creating a USB keychain that holds stored passwords on a data file. However, it has yet to be determined if users are comfortable with storing password information electronically as electronic storage ultimately makes it more accessible for hackers to gain access to this information. For some of these software programs, accessing the passwords does require that the user enter a master password, which makes it possible for a hacker to access many passwords by only cracking one.

As an alternative, security experts have claimed that more viable solutions can be found in biometrics. Biometric solutions include authenticating users with methods like eye scans, fingerprints and voice recognition. The biometric-based authentication applications consortium claims that biometric solutions are becoming more convenient and accurate for personal authentication. By tying authentication data to a particular individual, the user is authenticated securely without having anything to carry or remember. These solutions could be the most secure form of authentication, and have been used to grant access to highly secure physical environments within the government and military. However, applications in web environments still may be many years away from implementation.

While technological solutions are intended to aid password recall through allowing users to not enter passwords, they do nothing to actually help users remember passwords. Perhaps if we could reduce the mental workload and memory issues that exist in remembering passwords, then we would not need to turn to technological solutions nor force users to adopt and learn these new technologies. The next section will describe some of the formal observational research to help us understand the problem more clearly.

Formal Observational Research on Users and Passwords

Instead of looking towards technical solutions, many researchers have sought to understand how users are affected by authentication systems. These researchers suggest that system security in the past had been looked at entirely from a technical perspective, but little research had explored the human factors of security mechanisms. Past research which focused on authentication from a technical perspective has inevitably led to ineffective security mechanisms such as placing restrictions on passwords. In this section we will describe some of the formal observational research which looked at describing how users behave within these security systems.

Morris and Thompson (1979) conducted some of the earliest research describing how people choose passwords within authentication. They investigated how users chose passwords in a UNIX system when allowed to choose their own methods with no restrictions. The researchers found that a majority of passwords were a single word with 3 or less characters chosen. They also found that 86% of the passwords were familiar

terms that could be found with such reference tool as a dictionary or first name list. Their findings suggested that users choose passwords that are simple and easy to remember, but unfortunately also easier for hackers to decode.

In a similar study, Klein (1990) also showed that users choose passwords that are easy to remember and are generally a small subset of the full range of all possible passwords. For example, a password composed of any of the 26 characters in the American alphabet and the 10 digits within the Arabic numeral system can yield over 44 billion permutations within a case sensitive 6 character-based password. However, users do not take full advantage of that list. DeAlvare (1988) later added that once a password is chosen, a user is unlikely to change it until it has been shown to be compromised. The behavioral observations in these early studies suggest that memory may be the main cause of the usability problem of passwords.

Adams, Sasse, and Lunt (1997) surveyed and interviewed participants from multiple corporations about their use of passwords and analyzed the problem of password memory qualitatively using the method of grounded theory (Glaser & Strauss 1967). The researchers found that many of the memory issues relating to password authentication were linked to both the number of passwords and the frequency of password use. That is, password recollection decreased as the number of passwords a user had to remember increased and/or if the frequency of use of a particular password decreased. Therefore, the more often a user re-enters a particular password, the easier it is to remember the password. Similarly, the more passwords a user has in his/her lexicon of passwords, the harder it is to remember the correct password for each specific application or web site.

They observed that many users have to remember multiple passwords for different applications or because security mechanisms forced users to change their passwords periodically. This led to common behaviors such as users writing down passwords, choosing simple, easy to remember passwords, or creating multiple passwords that are similar to one other (name1, name2, name3).

This observational research suggests that memory is the main cause for the usability problems surrounding password authentication. Users choosing passwords with few characters, using easy to remember words and phrases, and displaying a reluctance to change passwords suggests that passwords are creating challenges on a user's memory. To understand how we can properly improve password memory, it is important that we understand the theories of how and why we forget information. In the next section we will investigate possible theories of why users forget passwords.

Human Memory: Why Do We Forget?

In this section we will briefly inspect human memory, which is at the heart of the problem. While the subject of human memory and learning compose of many topics, we will focus on why people forget and what factors and theories could address why users forget their passwords.

Before people can retrieve memories, they must encode them first. The encoding of memory goes through two storage processes. Information is first stored in working memory, and with learning and training is then stored into long term memory. Within the working memory storage process, information is coded into three core components

(Baddeley, 1995). The first component represents words and sounds that are stored in the phonological store. Verbal information can then be rehearsed vocally through the articulatory loop. The second main component represents visual information which is stored in the visuospatial sketchpad. The last component is the central executive which assigns attentional resources to the other components. Empirically it has been shown that the verbal and spatial codes do not compete for the same pool of resources (Brooks 1968). Thus, two tasks can be performed more efficiently if they are a combination of verbal and spatial codes than if they are both verbal or both spatial. Through the successful encoding of memory, we are then able to properly recall memory at a later time.

After memory is stored, we need to retrieve this information when required. However, retrieval is not always simple and many times, such as when users forget internet passwords, we fail altogether to retrieve needed information. Cognitive psychologists have developed many theories around why people forget. One theoretical argument suggests that retrieval is unsuccessful if the information is not rehearsed. Through rehearsal we are able to increase the probability that information transfers into long term memory (Atkinson & Shiffrin 1968). While simple repetitious behavior (e.g. repeating a phone number over and over) does help in remembering, often it is more elaborative rehearsal which can store information more deeply in memory and make that information easier to recall (Craik & Lockhart 1972). Elaborative rehearsal stores information more permanently in memory through using imagery, mnemonic elaboration, or organizing and structuring the target information meaningfully. For example, a

mnemonic technique called the “method of loci” involves associating items to be remembered with distinctive locations (Groninger, 1971). When recalling the items, one takes a mental walk to and between those associated locations.

In the topic of password authentication, rehearsal may be playing a roll as password forgetting relies on the frequency of password usage (Adams, et al. 1997). Through the process of using a password more often, that password is consequently rehearsed and creates an easier retrieval within long term memory.

A second theoretical aspect of forgetting is interference. Interference theories have proposed that people forget information because of competition from other material (Bjork 1992). Often this has been shown through paired-associate learning (Postman & Underwood 1973). Through pairing groups of words together, psychologists have shown that prior information can interfere with the ability to remember new information (proactive interference). Conversely, new information can interfere with the ability to remember old information (retroactive interference).

Interference may also be a factor when remembering passwords as the ability to remember a login password was shown to be affected by the number of passwords a user has to remember (Adams et al. 1997). As the number of passwords a user must remember increases, those passwords may come to interfere with each other such that a user confuses which password to use on which web site or application.

More recent theories have moved from the notion that people forget or lose memory information to theories that people simply have difficulty retrieving the information from long term memory. Cognitive Psychologists argue that trouble in

accessing information to be remembered will persist until an effective retrieval cue is presented; a cue which helps “locate” the information. A good retrieval cue has been described as one that is consistent with how the information was originally encoded (Tulving & Thompson 1973). Thus, if the sound of the word was emphasized during encoding, then an effective retrieval cue should emphasize the sound of the word. Likewise, if the meaning of the word was emphasized during encoding, then semantic cues should increase retrieval of the information. The principle that an effective cue is dependent on how the information is processed is known as encoding specificity. With the notion of encoding specificity, we see that information is stored not in isolation but in a much richer memory representation which includes extra information available during encoding. The lack of appropriate retrieval cues is a major cause of retrieval failure in human factors systems (Wickens & Hollands 2000), and we could include the current problem of recalling passwords within authentication.

Encoding specificity and retrieval cues fall under a broader construct known as context-dependent memory. Context-dependent memory stores contextual information along with the memory target such that contextual cues can be used to help retrieve information (Smith 1994). Context can refer to anything that surrounds the information to be remembered. Context could be meaningful in nature such as encoding information deeply through associations (i.e., using imagery). Context could also be spatial or temporal, such that it is information that is not obviously related to items in a memory test (i.e., the physical environment in which memory is encoded). This is called incidental context. One form of incidental context, known as intrinsic context, has been

shown to be powerful in recognition memory (Geiselman & Bjork 1980). Intrinsic context is incidental information, such as the color and font of target words, which affects memory during testing. For example, within computing systems, it has been empirically shown that users are prone to committing errors if the display location, color, and shape of numbers which are typed on a keyboard differ from what users have been trained to use (Wright & Shea 1991). As it relates to password memory, the environment within the login screen could be providing context, and cues within that environment could be utilized to aid in memory retrieval.

The study of forgetting has been extensive and suggests that the lack of rehearsal and the interference between similar items can both effect recall success. Observational studies on password usage have shown similar effects noting that the frequency of password usage (rehearsal) and the number of passwords one must remember (interference) are correlated to forgetting passwords. Further theories explain that people do not necessarily forget or lose memory, but have difficulty retrieving memory. Information, whether verbal or spatial, is encoded into memory along with other contextual information. When contextual information is associated with the target memory, then contextual cues can be used to stimulate memory and improve recall. We now turn towards describing the experimental research on authentication which has attempted to alleviate memory issues.

Experimental Research on Password Authentication

This section will explain what experimental research has been conducted on password authentication which has looked at improving password recall. Most of the experimental research on password authentication has explored alternative solutions and compared these solutions to the current style of character-based authentication.

Dhamija (2000) addressed password authentication problems by replacing characters with pictures. This research led to the Dejavu project which attempted to create a new form of password authentication using pictures, pointing out that people are much better at remembering images than characters (Standing 1973). In this study, the researchers compared the 1-week recollection of 4 digit pins, 6 character passwords, and image portfolios consisting of either 5 random art images and 5 photographs. The random art images were images with no coherent form or representation, while the photographs represented real world images that were expected to be familiar to participants (e.g. the Golden Gate Bridge). Results showed that PINs and character-based passwords had a lower performance by generating a greater percentage of failed logins. Therefore, images may prove to be easier to remember than traditional methods of PINs and character-based passwords. Qualitative results also showed that participants found the image based passwords easier to remember than character-based passwords. Looking at the difference between random art images and photos, the researchers found that it took longer for participants to remember the random art images than the photos. This suggests that users are better at recognizing photos than abstract images.

Goldberg, Hagman, and Sazawal (2002) also attempted to take a graphic approach to addressing users' failure to remember passwords by developing an authentication process called Passdoodle. Passdoodle is a password authentication method in which a user draws their password instead of entering an alphanumeric password. The password, thus, becomes a sketch the user makes. However, upon testing this method, the researchers found no difference in memory success between the sketches and alphanumeric character passwords. The main failure was that Passdoodle required participants to replicate the sequence of strokes used to create the sketch. Results showed participants failed in replicating the exact stroke sequence they previously created. However, the sketches participants made during recall did visually represent the password image. Thus, while participants could not effectively replicate the exact motion of creating the sketch, they appeared to have a more accurate mental picture and concept of the sketch.

Lu and Twidale (2003) looked at ways to reduce password forgetfulness by allowing the login and password to be semi-public. A system called MiFA (Minimal-Feedback Hints for Remote Authentication) was employed which allowed the user to choose a small number of password characters to display on screen while logging into a website. Thus, as a memory cue, part of the login and password was exposed to the participants. Pilot testing results showed MiFA-hinted passwords proved more effective than no hints at all.

In summary, these experiments have investigated the issue of increasing password memory through alternative methods. However, little has been done to increase the

familiar and currently established character-based authentication. MiFA-hinted passwords show promise as memory cues are important to retrieving passwords, however security risks are questionable if these MiFA hint cues are too exposing and could allow a hacker to guess the password. More secure modifications on current character-based passwords will be an important area to explore.

The Present Study

The present study explores how we can improve the character-based password authentication scheme. By analyzing principal memory research, we found that contextual retrieval cues are necessary in situations when there is a failure to retrieve information (Tulving & Thompson 1973). The present study analyzed if retrieval cues in the login environment can aid in the recall of character-based passwords.

There are different types of retrieval cues that can be utilized; however, this study focused on visual cues. There are several indications that choosing a visual cue could be beneficial. From an encoding perspective, it may be easier for users to encode a visual cue along with the character password as the two codes (verbal password and spatial cue) will not compete for resources while in working memory (Baddeley, 1995). From a security perspective, we must create a cue that can only be useful to the individual user and that separate users can not use the cue to help guess the password. A visual retrieval cue may be more secure as the associations only make sense within the mind of the individual user.

Building from prior experimental designs and their use of visual images as passwords, we looked at two different types of visual cues. One is an image cue, which is meaningful and represents objects that exist in the real world. The second is a pattern cue which is abstract graphic with no meaning. This factor is similar to the condition used within Dhamija's study (2000).

These visual cues were encoded at an explicit level. Thus, participants were told to use the images to help remember their password. By encoding at an explicit level, we attempted to achieve a deeper level of processing which should increase memory performance (Craik & Lockhart 1972).

The next section will describe more specifically the experimental design. We will define the procedure for the experiment, the independent variables, the dependent measures, and our hypothesis.

METHODS

Independent Variables

This experiment explored whether a visual cue can improve the memory performance of a character-based password. The independent variable under question had three levels: a visual image cue, a visual pattern cue, and a baseline condition which has no visual cue at all. Thus, there were three main conditions under comparison.

Comparisons were made within subjects and two data points were collected under each condition. Thus, each participant recalled two passwords under the visual image cue condition, two passwords under the visual pattern cue condition, and two passwords under the baseline. With 24 participants, this yielded a total of 144 trials (48 baseline trials, 48 pattern cue trials, 48 image cue trials).

To properly test if a cue had been learned, we also tested with the cue absent. If a cue is effectively encoded with an object and therefore increases memory performance during recall, then we would expect a decrease in recall performance if the cue is removed from the object during recall (Smith 1994). Thus, we designated 25% of the visual cue trials to display a cue (image or pattern) during encoding but not display that cue during recall. We labeled these absent cue trials. With 24 total absent cue trials (12 image cue trials and 12 pattern cue trials), we assigned each of the 24 participants one absent cue trial.

Dependent Measures

During password recall, two main dependent measures were collected. The first dependent measure is password success; was the participant able to recall the correct

password? The second dependent measure is password entry time; the amount of time, in seconds, it took a participant to enter their password. In addition to these measures, a post test survey collected information on participants' password behavior, predictions of recall success, whether participants felt the picture cues helped them remember their password, and if participants could match passwords to sites or pictures. See appendix B for the post test survey. Finally, participants were asked to recall the password a week after the first test for measuring long term recall performance. See appendix H for table of independent variables and dependent measures.

Participants

Twenty-four participants were recruited from San Jose State University Psychology 1 subject pool. Participants received research credit for their participation.

Visual Cue Stimuli

Two types of visual cues were used: images and patterns. Images are visual cues that represent real word objects. Image cues have the visual rendering of a photograph and no two images represent the same object. Patterns, on the other hand, are abstract visual cues that lack any semantic meaning. Both types of visual cues were selected from an online image database found at www.office.microsoft.com. All visual cues were presented in shades of gray to decrease any confounds created by color, and were displayed at 200x100 pixels. Four different image cues and four different pattern cues were shown to the 24 participants. The use of each image was rotated such that each

image was used equally within the experiment. This was deemed necessary to reduce any confounds that any one cue might increase memory over another.

Login Name and Passwords

The login name was consistent throughout the whole test: student@sjsu.edu. Passwords were six characters long, comprised of one letter, two digits, and a three character nonsense word. Passwords were arranged such that each had four chunks of information (e.g. e5fex4 and dev9s7). Passwords were also rotated between sessions so that each password was used equally within the experiment. This reduced any confounds caused by the ease of remembering one password over another. See appendix E for a list of the passwords.

Procedure

Participants were greeted by the experimenter and given a consent form. Participants were then seated at a computer and provided with a general introduction and overview. The experimenter explained to participants that they would simulate buying items online on six e-commerce sites.

Upon arriving at each site, participants encountered a login screen. Each login screen contained one of the three conditions: visual image cue, visual pattern cue, and the baseline. The participants were then presented with a login name and password. The login name remained consistent between each site, however the password was unique under each site condition. Participants were told that they would be required to

remember the password at a later time. If participants were under the login conditions of a visual image cue or a visual pattern cue, then participants were also given additional instructions to use the visual cue to help remember their password. See appendix G for examples of the login screen.

Participants then continued to shop online on the site and were given products to find. See appendix D for the list of products. Each product was specific and could only be located by reading the product description, and participants were instructed to not use the search box to find the items. This was intended to increase the difficulty of the task, which we believe would then decrease verbal rehearsing. Participants were also instructed to focus their attention on finding these products and to avoid rehearsing the passwords repetitiously within their heads.

After the participant spent 5 minutes looking for an item, participants were stopped by the facilitator and asked to re-login to the site. It is at this point that the dependent measures were collected and the test for recall occurred. There was thus a 5 minute gap between presentation and recall. All passwords were accepted even if the password was not correct and participants were not able to reenter their password if they made a mistake. This process repeated for the remaining sites, such that all 6 sites were experienced by participants.

After the session, participants were given a questionnaire inquiring about their general usage and memory of internet passwords and if they felt the picture cues helped them to remember their password. Participants were also asked to predict their recall

success and asked to match a list of passwords against a list of sites and a list of recall cues. See appendix B for the post test survey.

1 week from the test session we tested the long term effects of the visual cues. Participants were sent an email, asking them to recall their passwords through a recall test administered online. In this recall test, participants were asked to login to each site consecutively for all 6 sites. Participants were not told they would have to remember their password a week later in order to prevent rehearsal within the one week time period.

Additional Experimental Controls

To reduce confounding factors, the experiment was manipulated as follows: The most important control was to insure the stimuli materials were presented equally among all participants. Thus, the six passwords, the four image cues, and the four pattern cues were organized and rotated between participants such that each password was matched an equal number of times with each visual cue. In this experiment, password-cue pairs occurred twice among the 144 trials. Secondly, 4 randomly-selected Latin Squares were utilized to assign the order presentation of each condition throughout the 24 participants, thus reducing any order effects. Finally, sites were organized across participants as each site was assigned to each condition equally. In this experiment each site was assigned to a condition 8 times.

Hypotheses

Our main hypothesis was that the visual cue conditions should yield improved recall over the baseline condition. In addition, we expected the absent cue conditions to yield poorer recall. We also expected the visual image cues to yield higher recall success over the visual pattern cues. This would be consistent with Dhamija's (2000) findings that pictures were easier to recall than patterns. Finally, we expected these effects to be consistent with the long term tests.

RESULTS

Analysis within this section includes data collected from the immediate password recall trials, the post test survey, and the 1 week password recall trials. The primary measure, password recall success, was analyzed using a Chi-Square analysis. A General Linear Model was constructed for analyzing multiple levels of password recall time. Level of significance for this study was defined to be $\alpha \leq 0.05$.

Due to technical difficulties, 9 total data point trials were thrown out (4 image trials, 3 pattern trials, and 2 baseline trials). These difficulties came from internet instability within the testing environment, such that participants were not able to browse websites or login to sites as they would under normal conditions. Data points under these instances were thrown out. This discrepancy is represented within all the tables, as the total trial count is 135 instead of 144. Similarly, 6 participants who were solicited through email 1 week later, refused to take the 1 week recall test. This discrepancy is also represented within the 1 week recall data as the total trial count is 107 instead of 144.

Immediate Recall Test: Password Recall Success

The first result we will inspect is the immediate password success. This data describes whether a participant was able to enter the correct password after spending five minutes browsing for items on each site.

Within immediate recall, we first compared recall success between conditions which provided a recall cue on the login screen and those that did not (the baseline

condition). Results, as shown in Table 1 and Figure 1, showed a main effect between the conditions, $X^2(2, N = 113)$, $p \leq .05$, where the recall success rate for login screens with cues was greater than the baseline.

We next inspected the recall success between the four conditions: image recall cues, pattern recall cues, baseline recall cues, and absent cues (passwords encoded with a cue but not shown a cue during recall). Results, as shown in Table 2 and Figure 2, found significant effects between the four conditions, $X^2(4, N = 137)$, $p \leq .05$.

Further Chi-Square analyses were made between each of the conditions. Results showed that the Image Cue condition had a statistically significantly greater success rate (68.8%) than the Baseline (41.3%), $X^2(2, N = 78)$, $p \leq .05$. The Image Cue condition also had a statistically significantly greater success rate over the Absent Cue condition (33.3%), $X^2(2, N = 56)$, $p \leq .05$.

Likewise the Pattern Cue condition had a statistically significantly greater success rate (77.1%) than the Baseline (41.3%), $X^2(2, N = 81)$, $p \leq .05$. The Pattern Cue condition also had a statistically significantly greater success rate over the Absent Cue condition (33.3%), $X^2(2, N = 59)$, $p \leq .05$ conditions.

No statistical difference was found between success rates for the Image Cue condition (68.8%) and the Pattern Cue condition (77.1%) nor between success rates for the Baseline condition (41.3%) and Absent Cue condition (33.3%).

We also compared the recall success between the absent cues of images and the absent cues of patterns as seen in Table 3 and Figure 3. While the absent cues of images

showed a slightly higher recall success rate (41.7%) than the absent cues of patterns (25%), no statistically significant effect was found.

Table 1

Immediate password recall success between all recall cues and the baseline

Condition	Total Trials	Trial Frequency		Trial Rates	
		Successes	Failures	Success Rate	Failure Rate
All Cues	67	49	18	73.1%	26.9%
Baseline	46	19	27	41.3%	58.7%

Figure 1. Immediate password recall success between all recall cues and the baseline:

This data describes whether a participant was able to enter the correct password after spending 5 minutes browsing for items on each site. This figure represents the comparison between all recall cues and the baseline.

Table 2

Immediate password recall success between conditions

Condition	Total Trials	Trial Frequency		Trial Rates	
		Successes	Failures	Success Rate	Failure Rate
Image Cues	32	22	10	68.8%	31.2%
Pattern Cues	35	27	8	77.1%	22.9%
Baseline	46	19	27	41.3%	58.7%
Absent Cues	24	8	16	33.3%	66.7%

Figure 2. Immediate password recall success between conditions: This data describes whether a participant was able to enter the correct password after spending 5 minutes browsing for items on each site. This figure represents the comparison between all 4 main conditions: image cues, pattern cues, baseline, and absent cues.

Table 3

Immediate password recall success between absent cues

Condition	Total Trials	Trial Frequency		Trial Rates	
		Successes	Failures	Success Rate	Failure Rate
Absent Cue – Image	12	5	7	41.7%	58.3%
Absent Cue – Pattern	12	3	9	25%	75%

Figure 3. Immediate password recall success between absent cues: This data describes whether a participant was able to enter the correct password after spending 5 minutes browsing for items on each site. This figure represents the comparison between absent cues of images versus absent cues of patterns.

Immediate Recall Test: Password Recall Time

The next data point of inspection is the time to recall passwords. This is defined as the time that it took a participant to enter a password the moment they arrived on the login screen until the moment they submitted their password. We separated the comparisons between recall times of successfully entered password trials and failed password trials. This was to account for conditions with higher recall success rates, as shown in the prior results. A 2x4 General Linear Model was constructed to test for any effects within cue conditions (image cues, pattern cues, baseline, and absent cues), within trial types (successful trials and failed trials), and test if there is an interaction effect between conditions and trial types.

The data, as shown in Tables 4 and 5 and Figure 4, shows that between cue conditions under successful trials were relatively similar with absent cues yielding the shortest mean recall time ($M = 9.746$ seconds) and the baseline yielding the longest mean recall time ($M = 12.32$ seconds). Comparisons between mean failed trial times were more variable with the baseline yielding the lowest time ($M = 14.99$ seconds) and the pattern yielding the highest ($M = 22.30$ seconds). However, high variances within both successful and failed recall trials led to no main effects between conditions for recall times, $F(3, 129) = 0.45$, $p = 0.714$.

Comparisons between successful trials and failed trials showed a main effect, $F(1, 129) = 16.54$, $p \leq .05$, where the mean recall time for successful trials was shorter ($M = 10.78$) than the mean recall time for failed trials ($M = 17.95$).

Further analysis between cue condition and trial type showed no interaction effect, $F(3, 129) = 1.45$, $p = .231$. From an interaction plot, shown in Figure 5, we suspect the baseline condition as the key condition causing a small p-value in the statistical test for an interaction effect. We suspect this because of the low difference between the baseline mean recall time under successful trials ($M = 12.32$ seconds) and failed trials ($M = 14.99$ seconds).

Table 4

Immediate password recall times between conditions for successful trials

Condition	Successful trials		
	Total Trials	Mean Time (seconds)	Standard Deviation (seconds)
Image Cue	22	10.23	4.64
Pattern Cue	27	10.56	4.91
Baseline	19	12.32	8.21
Absent Cue	8	9.746	4.44

Table 5

Immediate password recall times between conditions for failed trials

Condition	Failed trials		
	Total Trials	Mean Time (seconds)	Standard Deviation (seconds)
Image Cue	10	19.07	11.76
Pattern Cue	8	22.30	22.74
Baseline	27	14.99	8.90
Absent Cue	16	18.91	12.60

Figure 4. Immediate recall time for both successful and failed trials between conditions:

This data describes the time it took a participant to enter a password the moment they arrived on the login screen until the moment they submitted their password. This figure compares all four main conditions for both successful recall and failed recall trials.

Figure 5. Interaction plot for immediate recall times: This data describes the time it took a participant to enter a password the moment they arrived on the login screen until the moment they submitted their password. This figure explains the interaction between all four main conditions and for both successful recall and failed recall trials. This figure shows that the baseline condition is tending towards causing an interaction between cue condition and trial type.

One Week Recall Trials: Password Recall Success

Recall success was tested one week from the study, where participants were emailed a link to the recall test and asked to take a recall test online. Overall, password success in the one week recall was poor, yielding no success under all conditions.

In reaction to the lack of success, we calculated partial success of passwords. An individual trial was defined as a partial success if the participant was able to correctly recall at least 50% of the characters (3 or more characters of a 6 character password) in correct consecutive order. For example, if the password target was e5fex4 and the recall entry was 3fex4w, then the entry would be considered a partial success because they correctly recalled 4 characters (fex4) in consecutive order. However, the recall entry of 3xf54 would not be considered a partial success; despite the entry including 4 characters of the correct password, no 3 characters were in the correct consecutive order.

Table 6 and Figure 6 show the results for partial success. All four partial success rates were quite low, with the Image Cue condition yielding the greatest partial success rate (13%) and the Baseline yielding the lowest with no partial success (0%). However, a Chi-Square analysis showed no statistically significant effects.

Table 6

One week password recall partial success between conditions

Condition	Total Failure Trials	Trial Frequency		Trial Rates	
		Partial Successes	Complete Failures	Partial Success Rate	Complete Failure Rate
Image cue	23	3	20	13%	87%
Pattern cue	29	1	28	3.4%	96.6%
Baseline	36	0	36	0%	100%
Absent Cue	19	1	18	5.3%	94.7%

Figure 6. One week password recall partial success between conditions: This data describes the recall success tested one week from the study, where participants were emailed a link to the recall test and asked to take a recall test online. This figure represents the comparison between all 4 main conditions.

One Week Recall Trials: Password Recall Time

The time for failed recall entries was only calculated, due to the lack of success, and is shown in Table 7 and Figure 7. Four trials with recall times greater than 60 seconds were removed as outliers. Results were similar to immediate recall where the baseline condition yielded the lowest failure time ($M = 12.34$ seconds) and pattern cue condition yielded the highest ($M = 18.65$ seconds). However, a statistically significant effect was not found.

Further analysis was conducted comparing 1 week password recall time within failed cue trials between all cue conditions (images and patterns) and the baseline. Results are shown in Table 8 and Figure 8, where failed cue trials yielded longer mean recall time ($M = 16.90$ seconds) than the baseline ($M = 12.34$ seconds). This difference approached statistical significance, $F(1, 84) = 2.75$, $p = 0.10$.

Table 7

One week password recall times

Condition	Trials	Failed trials	
		Mean Time (seconds)	Standard Deviation (seconds)
Image cue	23	14.79	12.40
Pattern cue	28	18.65	14.48
Baseline	35	12.34	10.80
Absent cue	17	15.78	12.67

Figure 7. One week password recall times between conditions: This data describes the time it took a participant to enter a password tested one week from the study. Since there was no success, this data only represents recall time for failed trials. This figure represents the comparison between all 4 main conditions.

Table 8

<i>1 week password recall times between cues and no cues</i>			
Condition	Trials	Failed trials	
		Mean Time (seconds)	Standard Deviation (seconds)
All Cues	51	16.90	13.59
Baseline	35	12.34	10.80

Figure 8. One week password recall times between cues and no cues: This data describes the time it took a participant to enter a password tested one week from the study, where participants were emailed a link to the recall test and asked to take a recall test online. Since there was no success, this data only represents recall time for failed trials. This figure represents the comparison between all cue conditions and the baseline.

Post Test Survey

After completion of tasks, a survey was given to participants. The post test survey asked participants: 1) whether or not participants felt the picture cues helped them remember passwords, 2) to predict which sites they correctly recalled the passwords of, 3) to match a list of passwords to a list of sites and a list of cues, 4) whether or not participants felt the picture cues helped them remember their password, and 5) share their general behaviors regarding internet passwords. The post test survey can be found in appendix B.

Qualitative results showed that 80% of the participants did not feel the picture cues helped to recall their passwords. Most respondents commented that the pictures had no relationship to the password and thus they could not make any associations between the two. Below is a sample of the comments:

- “I didn't see a connection between the picture and password”
- “The picture had nothing to do with the password”
- “Pictures had no relevance to the password. They were not meaningful to me”

Further analysis compared a participant's subjective response on whether the cue was helpful to the participant's actual recall success under cue conditions. Results show that there was no correlation between recall success under a cue condition and a participant perceiving that success, $r = .008$.

Participants were asked to predict which sites they remembered the passwords correctly and which sites they did not. On average, participants were able to correctly predict whether they were successful or not for 52% of the trials.

The post test survey also measured recognition between matching passwords with sites and matching passwords with recall picture cues. Results, Figure 9, show that participants were more successful in matching passwords to the recall picture cues ($M = 51.04\%$) than matching passwords to sites ($M = 36.11\%$). This effect approached statistical significance, $F(1, 46) = 3.18, p = 0.08$. Further analysis investigated if there was any difference between image cues and pattern cues within matching success. Results are shown in Figure 10. While images cues ($M = 56.2\%$) had a slightly higher mean matching success rate over pattern cues ($M = 45.8\%$), there was no statistical difference between image cues and pattern cues within matching success, $F(1, 46) = 0.70, p = 0.40$.

Other questions in the post test survey polled participants regarding their past behavior regarding internet passwords, shown in Figure 11. Notably, 41% of participants indicated they used 5 to 10 unique web sites requiring passwords, 25% indicated they used 1 to 5 sites, and the remaining 44% logged into 11 or more sites requiring passwords. Participants also indicated that they logged into an average of 5 sites per day.

Further behavior questions were represented as Likert scales and are shown via Figures 12 through 15. More notably from this data we see that participants tend to use few unique passwords (Figure 12), participants are more likely to create a new account

than stop using a website (Figure 13 and Figure 14), and participants tend to not change or rarely change their passwords (Figure 15).

Figure 9. Matching success between web sites and recall cues: A post test survey measured recognition between matching passwords with sites and passwords with recall picture cues. This data compares the mean matching success rate between matching passwords to sites versus recall cues.

Figure 10. Matching Success between Image Cues and Pattern Cues: A post test survey measured recognition between matching passwords with recall picture cues. This figure compares the mean success of correctly matching passwords to images cues versus pattern cues.

Figure 11. Frequency of sites requiring passwords: From a post test survey, this graph represents the frequency of participant responses to a question on how many sites participants use which require a name and password.

Figure 12. Unique passwords per site: From a post test survey, this graph represents the frequency of participant responses to a question on how many unique passwords participants have for the websites they use.

Figure 13. Frequency of new account creation for forgotten passwords: From a post test survey, this graph represents the frequency of participant responses to a question on how often participants create a new account when they forget a web site password.

Figure 14. Frequency of web site abandonment due to forgotten passwords: From a post test survey, this graph represents the frequency of participant responses to a question on how often participants have stopped using a web site because they forgot their password.

Figure 15. Frequency of changing passwords: From a post test survey, this graph represents the frequency of participant responses to a question on how often participants change their password for an individual site.

DISCUSSION

Support for Recall Cues within the Login Environment

Several data points lead us to conclude that recall cues were helpful during immediate recall. First and foremost, immediate recall results showed that both images and patterns had a statistically significant higher success rate than the baseline. A low success for the absent cue trials also supports the positive effect of picture cues, as a cue that is encoded within memory should decrease performance if that cue is removed during recall (Smith 1994).

Another support for a positive effect of picture recall cues can be inferred from the password recall time. The main effect of failed trials yielding longer recall times than successful trials could be due to the memory scanning process theory of self-terminating search (Ashcraft 1994). This theory states that we search for remembered items within memory serially, stopping when we find the correct answer. Thus, the failed trials are longer as participants spent more time searching through their memory to find the correct password. While there was no main effect in recall time between conditions, the baseline condition is showing the tendency to create an interaction effect. This is due to a small difference in mean recall time between the successful trials and failed trials within the baseline condition. Thus while the other three conditions show longer mean recall times for failed trials than their respective successful trials, the baseline condition shows a relatively small difference. This suggests potentially only those conditions encoded with a recall cue create longer recall time for failed attempts. Similar results were found

in the 1 week recall test, where recall times for failed results in all cue conditions were longer than the baseline condition.

A longer time to enter a failed password suggests that despite their inability to recall the correct password, these participants took an extended period of time in an attempt to recall what they hoped would be the correct password. This increased motivation for attempting to recall the correct password could be due to a heightened sense of recalling the correct password. This is similar to the “tip-of-tongue” phenomena, which notes that participants within this state have partial access to the information necessary to recall correctly, and are thus further down the path of successful recall (Brown and McNeill 1966). Therefore, we can infer that those conditions with a longer recall time for failed passwords promote a higher ability to recall passwords. Given the results of a potential emergence of an interaction effect between cue condition and trial type, there is the possibility that those conditions encoded with cues yielded longer mean recall time for failed trials due to a heightened sense of recalling the correct password.

A final support for picture cues comes from the recognition survey which showed that participants were more successful in matching the correct password to a picture cue, than to the site itself. This suggests that the cue and environment may be more important in recognizing the correct password than the name of the site.

Incidental Contextual Cues

Although recall cues were shown to be helpful in recalling passwords, further results showed that this effect was not explicitly conscious to participants. A majority of participants (80%) felt that the recall cue did not help them remember their password. Participants also showed a poor prediction of their own success, as they were only able to correctly predict if they chose the correct password an average of 52% of the trials. Therefore, although a picture cue did indeed have an effect, it was unnoticed by participants.

Our prior discussion of context-dependent memory may help further define the effect the pictures cues have within this experiment. Prior theories of context-dependent memory specify both meaningful context that is encoded through deep associations and relationships, and incidental context which is information that lies in the environment and is not obviously related to the recall items.

Within this experiment, meaningful context would have been achieved by participants' ability to make a strong association between the picture cue and the password. However, participants did not appear to make meaningful contexts, as qualitative feedback showed a majority of participants did not feel the pictures were helpful during recall and had difficulty making relationships between pictures and passwords. Also, had the effects been due to meaningful contexts, we would have expected images to have a higher recall than patterns. Images have more inherent significance as they represent real world objects and we would thus expect image cues to be more successful in generating more in depth and meaningful associations than pattern

cues. However, the results showed otherwise, as images and patterns were not statistically significant from each other, and in fact pattern cues showed a slightly higher recall success rate than image cues.

Therefore, our results suggest that the effects of picture cues increasing recall performance may be one of incidental context rather than meaningful context. Recall cues did not improve performance as a result of participants developing explicit associations between the pictures and passwords. Instead, the visual environment of the login screen provided implicit recall cues. Within an explicit/implicit memory model we would suggest that these cues were encoded on an implicit memory level (Graf and Schacter, 1985). Explicit memory is explained as information that is available for conscious recollection that helps during a recall task. Implicit memory, on the other hand, is information that is not available for conscious recollection, but it too can increase recall performance. This helps explain why recall cues improved performance even though participants were not able to make meaningful associations between images or patterns with passwords.

Cue Limitations: Long Term Effects

Although recall cues helped, it was limited to only immediate recall. The cues did not have any lasting effect, as the 1 week recall test showed no success within all conditions. Partial success was greatest among images, however, not enough to be statistically significant. This could be because the passwords were given and not familiar to participants. Low long term success may also be due to participants not having a

chance to use the password repetitively, which has been found to increase the recall performance of passwords over time (Adams et al. 1997).

Consistency with Observational Research

The post test survey showed consistent results with prior observational research. Notable, a majority of participants had few passwords and tended to use a single password for multiple sites, which was similar to behaviors found by Adams et al. (1997). Also, participants tended to never or rarely change their password, which was similar to behaviors reported by DeAlvare (1988). Behaviors such as these confirm that our sample of participants have experienced similar problems in authentication recall as we would have expected.

Implications for Web Design

Results from this study suggest a powerful design tool through the use of recall cues. Incidental contextual effects found within this experiment suggest that the login page environment could be a powerful mechanism for helping users recall their internet passwords. In this experiment we found that login screens with a picture cue increased recall success more than having blank login screen with no cue. This could suggest that visually enhancing a login screen with visual imagery could help users remember their passwords. Perhaps this can be accomplished using specific cues, as shown in this study, or just creating a visually rich environment with which participants can make their own

incidental contextual cues. Potential solutions should be further researched in order to understand how cues can be used most effectively.

Limitations

There are a number of limitations associated in this study, to include: 1) long term recall effects and 2) use of unfamiliar passwords.

Participants were not told they would be tested for recall when sent the 1 week test. While this was intended to keep participants from rehearsing their passwords during the 1 week time span, it could have affected the success of password recall as participants could have assumed they would never need the password again and dumped their memory due to no motivation to remember. We suspect this may not be normal internet password behavior usage.

Another limitation is the type of password given to participants. Participants were purposefully given passwords which were unbiased and neutral. However, prior observational research has shown that these are the types of passwords which are not likely to be chosen by users. Thus, further research is necessary to determine if the effects from this study will be similar for passwords that are more meaningful or chosen by participants.

Further Research

Results from this study point towards several avenues for further investigation on how recall cues effect internet passwords. First, further experiments should explore the

effects of using passwords with more meaning. The passwords in this experiment were specifically chosen so as to not create any bias between participants. However, more ecologically valid passwords would include passwords which represent real word objects or concepts (first names, important dates, etc.). Further research should explore how login environment recall cues affect more meaningful passwords, including passwords chosen by participants.

Repetition of password usage was an important behavior in how people remember internet passwords. Further research should explore the effects of these cues when users continuously use passwords in long term contexts. Such research could lead towards more effective investigations towards recall within a longer time frame, such as after one week or a month.

Further analysis could dig deeper into how password recall is affected by cues in multiple short term trials. For example, further analysis could explore the effect of the absent cue condition on later trials where the picture cue is introduced again in a second recall trial. Analysis such as this could explore whether a visual consistency in login screens is important.

Finally, further manipulations of cues could be explored in much greater detail. In this experiment, we found that images and patterns were not statistically different in recalling passwords. However different aspects (color, size, and position) could be further explored. Furthermore, the method of cue could also be explored further, such as using audio cues or animated cues.

CONCLUSION

The growth of online systems and products has increased the number of passwords for the average user. Observational research has described user behaviors such as choosing passwords with few characters, using easy to remember words and phrases, and a reluctance to change passwords. Behaviors like these reflect the notion that passwords challenge a user's memory. Fundamental memory research suggests several theories to forgetting. One such theory explains that people do not necessarily forget or lose memory, but have difficulty retrieving memory (Tulving & Thompson 1973). Information, whether verbal or spatial, is encoded into memory along with other contextual information. When contextual information is associated with the target memory, then contextual cues can be used to stimulate memory and improve recall.

The present study investigated how we can improve the current and familiar character-based password authentication scheme by using retrieval cues in the login environment to aid in the recall of character-based passwords. We used both image cues, which was meaningful and represents objects that exist in the real world, and pattern cues which were abstract graphics with no meaning.

Results showed that visual cue conditions did yield improved recall over the baseline condition. However, there was no difference between image cues and pattern cues. Further qualitative results showed that participants did not find the picture cues helpful when recalling passwords as they could not make any associations between the picture cue and the password. The inability to make any strong associations leads us to believe that within the context-dependent memory framework, the cues in this experiment

were of incidental context rather than meaningful context. This suggests that although participants were not able to make associations between passwords and cues, the login page environment was a powerful catalyst for helping participants remember their passwords.

REFERENCES

- Adams, A., Sasse, M. A., Lunt, P. (1997) Making passwords secure and usable. In H. Thimbleby, B. O'Conaill & P. Thomas (eds.), *People & Computers XII (Proceedings of HCI'97)* (pp. 1-19). Springer.
- Adams, A., Sasse. (1999) Users Are Not The Enemy. *Communications of the ACM*. December 1999. Vol 42. No. 12.
- Ashcraft, M.H. (1994) Human Memory And Cognition. (pp. 168) New York, NY: Harper Collins.
- Atkinson, R.C., Shiffrin, R.M. (1968). Human memory. A proposed system and its control processes. In W.K. Spence & J.T. Spence (Eds.), *The psychology of learning and motivation: Advances in research and theory* (Vol. 2, pp. 89-195). New York: Academic Press.
- Baddeley, A.D. (1995). Working memory. In M.S. Gazzaniga et al. (Eds.), *The cognitive neurosciences* (pp. 755-784). Cambridge, MA: MIT Press.
- Biometrics Consortium. Retrieved March 20th, 2004, from <http://www.biometrics.org/html/introduction.html>

Bjork, R.A. (1992). Interference and forgetting. In L.R. Squire (Ed.), *Encyclopedia of learning and memory*. New York: Macmillian.

Brooks, L.R. (1968). Spatial and verbal components in the act of recall. *Canadian Journal of Psychology*, 22, 349-368.

Carroll, J.M (1996) *Computer Security* (3rd ed). Butterworth-Heinemann, MA.

Craik, F.I.M., Lockhart, R.S. (1972). Levels of processing: A framework for memory research. *Journal of Verbal Learning and Verbal Behavior*, 11, 671-684.

DeAlvare, A. M.(1988) A Framework for Password Selection. *Unix Security Workshop II*. Portland. Aug 29 - 30

Dhamija. (2000) Hash Visualization in User Authentication. *Proceedings of Conference of Human Factors in Computing Systems*. 2000. p. 279-280

Diaz, S. (2003, Sep). Password Overload. *SiliconValley.com*, Retrieved January 17th 2004 from <http://www.siliconvalley.com/mld/siliconvalley/6688853.htm>

Geiselman, R.E., Bjork, R.A. (1980). Primary versus secondary rehearsal in imagined voices: Differential effects on recognition. *Cognitive Psychology*, 12, 188-205

Glaser, B. and Straus A. (1967) *The Discovery of Grounded Theory: Strategies for Qualitative Research*. Chicago, IL: Aldine.

Goldberg G., Hagman J., and Sazawal V. (2002) Doodling Our Way to Better Authentication *Proceedings of Conference of Human Factors in Computing Systems*. 2002. p. 868-869

Groninger, L. D. (1971). Mnemonic imagery and forgetting. *Psychonomic Science*, 23, 161-163.

Klein, D. (1990). Foiling the Cracker: A Survey of, and Improvements to, Password Security. *Proceedings of the 2nd USENIX Workshop on Security*.

Light, A. (2003, Apr). Passwords demonstrably Weak Link in Secure Design. *UsabilityNews.com*, Retrieved January 17th 2004 from <http://www.usabilitynews.com/news/article1053.asp>

Lu, B and Twidale, M.B. (2003) Managing Multiple Passwords and Multiple Logins: MiFA Minimal-Feedback Hints for Remote Authentication. University of Illinois at Urbana-Champaign, Graduate School of Library and Information Science.

Morris, and Thompson. (1979) Password Security: A Case History. *Communication of the ACM*. November 1979 Vol 22. No. 11.

Nielson, J. (1995, Aug). Directions for Online Publishing. *Alertbox*, Retrieved December 22nd 2003 from <http://www.useit.com/alertbox/9508.html>

Nielson, J. (2000, Nov). Security & Human Factors. *Alertbox*, Retrieved December 22nd 2003 from <http://www.useit.com/alertbox/20001126.html>

Postman, L., & Underwood, B.J. (1973). Critical issues in interference theory. *Memory & Cognition*, 1, 19-40.

Research-Based Web Design & Usability Guidelines. (2003) Retrieved January 17th 2003, from <http://usability.gov/guidelines/designconsid.html>

Smith, S.M. (1994). Theoretical principles of context-dependent memory. In P.E. Morris, M. Gruneberg (Eds), *Theoretical Aspects of Memory*. (pg 168-195). London and New York: Routledge

Standing, L. (1973) Learning 10,000 pictures. *Quarterly Journal of Experimental Psychology*, 25, 207-222.

Tognazinni, B. (2003, Nov). Maximum Security. *AskTog*. Retrieved December 22nd 2003
from <http://www.asktog.com/columns/058SecurityD'ohlts.html>

Tulving, E., Thompson, D.M. (1973). Encoding specificity and retrieval processes in episodic memory. *Psychological Review*, 80, 352-373.

Wickens C. D., Hollands, J.G. (2000). *Memory and Training*. Engineering Psychology and Human Performance (pp. 281) New Jersey: Prentice Hall.

Wright, D.L., Shea, C.H. (1991). Contextual dependencies in motor skills, *Memory and Cognition*, 19, 361-70.

Appendix A

Agreement to Participate in Research

Responsible Investigator(s): Mark Wehner

Title of Protocol: Internet Password Behavior

1. You have been asked to participate in a research study investigating the purpose of the study is to determine the effects on Web Shopping.
 2. You will be asked to interact with different e-commerce sites and buy items. You will also be asked to memorize login passwords for completing these tasks. The tasks will be followed by a short survey.
 3. No risk to you during this session is anticipated.
 4. No discernable direct benefits to you will come from this research, although the information may be used to help make web pages easier to use.
 5. Although the results of this study may be published, no information that could identify you will be included.
 - 6 There will be no compensation for participation in this research.
 7. Questions about this research may be addressed to Mark Wehner (408) 349-6541. Complaints about the research may be presented to Dr. Kevin Corker, Director of the Graduate Program in Human Factors/Ergonomics, Industrial & Systems Engineering Department, College of Engineering, at (408) 924-3988. Questions about research subjects' rights, or research-related injury may be presented to Pam Stacks, Associate Vice President, Graduate Studies and Research, at (408) 924-2480.
 8. No service of any kind, to which you are otherwise entitled, will be lost or jeopardized if you choose to "not participate" in the study.
 9. Your consent is being given voluntarily. You may refuse to participate in the entire study or in any part of the study. If you decide to participate in the study, you are free to withdraw at any time without any negative effect on your relations with San Jose State University or with any other participating institutions or agencies.
 10. At the time that you sign this consent form, you will receive a copy of it for your records, signed and dated by the investigator.
- **The signature of a subject on this document indicates agreement to participate in the study.**

- **The signature of a researcher on this document indicates agreement to include the above named subject in the research and attestation that the subject has been fully informed of his or her rights.**

Signature

Date

Investigator's Signature

Date

Appendix B

Post-Test Survey

The following questions inquire about your interaction with passwords on internet. Please answer honestly, and only select one answer per question unless it is noted otherwise.

1. How many websites do you use which require a user name and password?

- A. 1-5
- B. 6-10
- C. 11-15
- D. 16-20
- E. 21 or more

2. How many times a day do you log into web sites with a login name and password?

3. How many unique passwords do you have for the websites you use? (circle the number)

1	2	3	4	5	6	7
Each website I use has a unique password			About ½ the websites I use have a unique password.			All the websites I use have the same password

4. How often have you created a new account when you forgot a web site password? (circle the number)

1	2	3	4	5
Never		Sometimes		All the time

5. How often have you stopped using a web site because you forgot your password? (circle the number)

1	2	3	4	5
Never		Sometimes		All the time

6. How often do you change your password for an individual site? (circle the number)

1	2	3	4	5
Never		Sometimes		All the time

7. Which of the following sites do you think you remembered your passwords? Check those which you believe you remembered your password successfully.

- ☐ www.Amazon.com
- ☐ www.CNET.com
- ☐ www.macys.com
- ☐ www.walmart.com
- ☐ shopping.yahoo.com
- ☐ www.outpost.com

8. Match the following passwords to each site: (place a letter in each field)

- A. 8h6zun
- B. bim4w3
- C. e5fex4
- D. 1g5cer
- E. dev9s7
- F. w9nat2

_____ www.macys.com
 _____ www.CNET.com
 _____ www.Amazon.com
 _____ www.outpost.com
 _____ shopping.yahoo.com
 _____ www.walmart.com

9. Match the following passwords to each picture: (place a letter below each picture)

- A. 8h6zun
- B. bim4w3
- C. e5fex4
- D. 1g5cer
- E. dev9s7
- F. w9nat2
- G. N/A I did not see this picture during the experiment.

10. Did you find the pictures helped you remember your password? Why or why not?

Appendix C

Task Protocol

Introduction (Read out loud to participants):

Welcome, and thank you for volunteering to participate in today's research. In this experiment, you will be performing 6 online shopping tasks and 6 different sites.

For each task, you will buy a specific items as specified on the task sheet <point out the sheet>. You will go through each item one by one, and when you feel like you have found the item that matches the description, let me know and then you can move onto the next item.

You will not actually be purchasing the items, but just finding these items. However, you will not be allowed to use the search box to find items.

In addition to browsing items online, you will also be asked to login to each site by providing a login name and password. You will use the same login name for each site: **student@sjsu.edu**. This will automatically display for you. However, you will be provided with a different password for each site you log into.

When you first login to the site, the password will be given to you on screen. Remember this password as you will be required to login to a site after finding the items to purchase. Also, some login screens will have a picture on the screen. I would like you to use this picture, as best you can, to help remember your password. Although you will be required to remember passwords, please try and focus on finding items and not repeating the passwords in your head.

Additional instructions will appear on screen. Please read each instruction carefully and thoroughly as you go through the experiment.

I will be close by to answer any questions and monitor the session.

Before we begin, do you have any questions?

Appendix D

Item Task Sheet

www.Amazon.com: Find these items:

- 100% cotton black sweater
- Cell Phone which has a camera and is “Blue Tooth” compatible.
- Book: “The Dark Tower” by Stephen King
- CD: “How dismantle and atom bomb” by U2

www.CNET.com: Find these items:

- Cannon Digital Camera which weighs less than 4 ounces.
- Mp3 player with a 1 year warranty
- Laptop computer which weighs less than 3 pounds and has a “track point”

www.macys.com - Find these items:

- King size pillow with a thread count greater than 400
- Knife set which includes a bread knife
- Pearl earrings for less than \$200.00

www.walmart.com – Find these items:

- Exercise bike which can monitor your heart rate
- 3 bulb floor lamp
- Pool table with leather pockets

www.shopping.yahoo.com – Find these items:

- Telescope which magnifies over 300x
- Pink roses with a teddy bear

www.outpost.com – Find these items:

- DVD player which also has a VHS tape deck, and can record DVDs.
- Flat panel TV which can be wall mounted.

Appendix E

Passwords

Password 1: e5fex4

Password 2: 8h6zun

Password 3: w9nat2

Password 4: dev9s7

Password 5: 1g5cer

Password 6: bim4w3

Appendix F

Picture Cues

Image Cues

Pattern Cues

Appendix G

Login Screens Encountered by Participants

Welcome to www.macys.com!

Before you can continue, you must sign in. Please enter your login name and password.

Please use the password: **e5fex4**

Remember this password as you will be asked to login to the site again later in this study.

There is a picture to the left. Use this picture to help remember your password.

Login Name student@sjsu.edu

Password

Login screen during presentation – image cue condition

Welcome to www.outpost.com!

Before you can continue, you must sign in. Please enter your login name and password.

Please use the password: **w9nat2**

Remember this password as you will be asked to login to the site again later in this study.

There is a picture to the left. Use this picture to help remember your password.

Login Name student@sjsu.edu

Password

Login screen during presentation – pattern cue condition

Welcome to www.amazon.com!

Before you can continue, you must sign in. Please enter your login name and password.

Please use the password: **8h6zun**

Remember this password as you will be asked to login to the site again later in this study.

Login Name student@sjsu.edu

Password

Login screen during presentation – baseline condition

Welcome to www.macys.com!

Before you can continue, you must sign in. Please enter your login name and password.

Login Name student@sjsu.edu

Password

Login screen during recall – image cue condition

Welcome to www.outpost.com!

Before you can continue, you must sign in. Please enter your login name and password.

Login Name student@sjsu.edu

Password

Login screen during recall – pattern cue condition

Welcome to www.amazon.com!

Before you can continue, you must sign in. Please enter your login name and password.

Login Name student@sjsu.edu

Password

Login screen during recall – baseline and absent cue conditions

Appendix H

Independent and Dependent Variables

Independent Variables	Trials Per Participant N=24 within subjects	Total Trials
Baseline	2	48
Image Cue	2	36 (12 of 48 trials displayed as absent cues)
Pattern Cue	2	36 (12 of 48 trials displayed as absent cues)
Absent Cue	1 image or pattern cue displayed as an absent cue	24
	6 trials per participant	144 trials total in experiment

Dependent Measures:

- **Recall success:** Whether the participant was able to remember their password.
- **Time to recover password:** Time, in seconds, which it took participants to remember their password after encountering the login screen.