Improving password cybersecurity through inexpensive and minimally invasive means: Detecting and deterring password reuse through keystroke-dynamics monitoring and just-in-time fear appeals

Password reuse—using the same password for multiple accounts—is a prevalent problem that can make even the most secure systems vulnerable. When passwords are reused across multiple systems, hackers may compromise accounts by stealing passwords from low-security sites to access sites with higher security. Password reuse can be particularly threatening to users in developing countries where cybersecurity training is limited and hackers perceive that these regions do not have programs to secure cyberspace or to enforce cybersecurity laws. This article proposes a two-pronged solution for reducing password reuse through detection and mitigation. First, based on the theories of routine, cognitive load, and motor movement, we hypothesize that password reuse can be detected by monitoring characteristics of users’ typing behavior (i.e., keystroke dynamics). Second, based on protection motivation theory, we hypothesize that providing just-in-time fear appeals when a violation is detected will decrease password reuse. We tested our hypotheses in an experiment and found that users’ keystroke dynamics are diagnostic of password reuse. By analyzing changes in typing patterns, we were able to detect password reuse with 81.71% accuracy. We also found that just-in-time fear appeals decrease password reuse; 88.41% of users who received a fear appeal subsequently created unique passwords, whereas only 4.45% of users who did not receive a fear appeal created unique passwords. Our results suggest that future research should continue to examine keystroke dynamics as an indicator of cybersecurity behaviours, and use just-in-time fear appeals as a method for reducing non-secure behavior. The findings of our research provide a practical and cost-effective solution to bolster cybersecurity through discouraging password reuse.

Keywords: password reuse; keystroke dynamics; protection motivation theory; just-in-time fear appeals; support vector machine; cybersecurity; developing countries

# Introduction

Global information and communication technology is rapidly growing ([Maurer, 2011](#_ENREF_40)); however, developing countries frequently lack adequate cybersecurity controls and opportunities to educate the public about cybersecurity[[1]](#footnote-1) ([Chen et al., 2006](#_ENREF_11)). Attackers (e.g., hackers, fraudsters) therefore target users from developing nations because they perceive that these regions do not have programs to secure cyberspace or to enforce cybersecurity laws ([Tagert, 2010](#_ENREF_57)). Through gaining unauthorized access to user accounts, these attackers commit cybercrimes (e.g., identity theft, theft of money, phishing, unauthorized access to organizational or governmental resources) or even cyber warfare against other nations—e.g., espionage, sabotage, denial of service attacks, and malicious code hosting ([Maurer, 2011](#_ENREF_40); [Tagert, 2010](#_ENREF_57)).

One common tactic leveraged to attack users is through exploiting password reuse—i.e., taking advantage of a user who has an identical password across multiple accounts ([Ives et al., 2004](#_ENREF_29); [Notoatmodjo & Thomborson, 2009](#_ENREF_45)). When password reuse occurs, hackers have the ability to steal credentials from one site (e.g., a low-security or fraudulent web site hosted in a developing country) and use these credentials to breach other sites, even those that have considerable cybersecurity controls in place ([Notoatmodjo & Thomborson, 2009](#_ENREF_45)). This phenomenon is often referred to as the ‘Domino Effect’—after the failure of the weakest system, other systems will follow, yielding new password information from which still more systems will fail ([Ives et al., 2004](#_ENREF_29)).

Despite the dangers of password reuse, it is very prevalent. A global study of over 500,000 users found that people, on average, access 25 password-protected sites using only 6.5 unique passwords, resulting in passwords being shared across 3.9 sites on average ([Florencio & Herley, 2007](#_ENREF_17)). Users suffer from ‘password-overload’ with over half of individuals surveyed admitting to having reused a password for highly-important accounts ([Notoatmodjo & Thomborson, 2009](#_ENREF_45)). Several potential solutions have been proposed to deter password reuse, such as password managers ([Gaw & Felten, 2006](#_ENREF_21)), alternative authentication methods ([Ives et al., 2004](#_ENREF_29)), and composition rules ([Campbell et al., 2011](#_ENREF_8)). Although some of these techniques have shown utility, particularly in an organizational setting, their public penetration is low because of high costs, mass-deployability issues, or technical limitations ([Bonneau et al., 2012](#_ENREF_4)). These problems are amplified in developing nations where cyber-infrastructure is poor, IT knowledge lags behind ([Carte et al., 2011](#_ENREF_9); [Pick & Azari, 2008](#_ENREF_50)), public/shared computer use is high ([Florencio & Herley, 2006](#_ENREF_16)), and financial resources are scarce relative to other nations ([Roztocki & Weistroffer, 2011](#_ENREF_53)) (see Table 1 in the literature review section for a more detailed discussion).

We propose a cost-effective methodology for mitigating password reuse by detecting when it occurs, and then displaying just-in-time fear appeals. By implementing these warnings on an “as needed” basis, we intend to target users who are likely reusing passwords while not inconveniencing those who are likely creating unique passwords. This can provide a cost-effective remedy that is feasible to implement in the developing world. In this article, we describe how password reuse can be identified by monitoring a user’s keystroke behavior (i.e., keystroke dynamics). We then explain why just-in-time fear appeals provided on an “as needed” basis will discourage password reuse. In summary, we help address the need to decrease password reuse by answering the following questions:

*RQ1. Can keystroke dynamics be used to predict if individuals are reusing passwords?*

*RQ2. Does providing just-in-time fear appeals help reduce password reuse?*

# Literature Review

Recognizing the dangers of password reuse, researchers have been challenged to better understand and create solutions to mitigate password reuse ([Ives et al., 2004](#_ENREF_29)). Table 1 reviews selected password reuse deterrence strategies identified in literature, and their applicability to the developing world. A suggested cause of password reuse is that users are often unaware of what constitutes good password practices ([Furnell, 2007](#_ENREF_19)). While previous studies have shown that training may increase awareness and thereby reduce password reuse ([Charoen et al., 2008](#_ENREF_10); [Ives et al., 2004](#_ENREF_29)), training alone is rarely sufficient. For example, in a developing world context, users in Nigeria who were given brief training on improving passwords by using mnemonics simply used easily-memorable, easily-hacked mnemonics rather than unique strong passwords ([Oghenerukevbe, 2010](#_ENREF_47)). Other research suggests that even if users know what constitutes good or bad password practices, they have little motivation to comply because they perceive little threat and do not want to be inconvenienced—users gravitate toward the path of least resistance ([Tam et al., 2010](#_ENREF_58); [Zhang & McDowell, 2009](#_ENREF_67)). One suggested way to overcome these limitations is through fear appeals ([Herath & Rao, 2009](#_ENREF_26); [Johnston & Warkentin, 2010](#_ENREF_32)). Fear appeals can be implemented to help increase users’ perceptions of the costs and dangers of reusing passwords ([Zhang & McDowell, 2009](#_ENREF_67)); the more probable people perceive that their accounts can be compromised, the less likely they are to reuse passwords ([Bryant & Campbell, 2006](#_ENREF_6)).

|  |  |
| --- | --- |
| Table 1. Examples of Password Reuse Deterrence Strategies | |
| **Password Reuse Solution** | **Effectiveness in Developing Nations** |
| Client-side password management systems ([Gaw & Felten, 2006](#_ENREF_21)) | Computer use often occurs on public computers and in computer cafés in developing nations where the use of password managers may not be feasible ([Florencio & Herley, 2006](#_ENREF_16)) |
| Composition rules / password requirements ([Campbell et al., 2007](#_ENREF_7); [Campbell et al., 2011](#_ENREF_8); [Keith et al., 2009](#_ENREF_34)) | While composition policies reduce the use of dictionary words and similar words, they do not normally reduce password reuse ([Campbell et al., 2011](#_ENREF_8)) |
| Alternative forms of authentication ([Ives et al., 2004](#_ENREF_29)), for example:   * neural networks ([Shouhong & Hai, 2008](#_ENREF_56)) * graphical passwords ([Biddle et al., 2012](#_ENREF_3)) * smart cards ([Hwang et al., 2010](#_ENREF_28)) * one-time passwords using specialized servers ([Huang et al., 2011](#_ENREF_27)) | Although useful in many organizational settings, these alternative forms of authentication have low public penetration because “none… retains the full set of benefits that legacy passwords already provide” ([Bonneau et al., 2012, p. 1](#_ENREF_4)). |
| Training ([Charoen et al., 2008](#_ENREF_10); [Ives et al., 2004](#_ENREF_29)) | Normally not sufficient alone to deter password reuse in developing nations ([e.g., Oghenerukevbe, 2010](#_ENREF_47)); there are limited opportunities to mass educate the public in developing nations ([Cone et al., 2007](#_ENREF_12)). |

Fear appeals are explained by a number of theories, protection motivation theory (PMT) being among the most developed ([Rogers, 1975](#_ENREF_51); [Rogers, 1983](#_ENREF_52)). Johnston and Warkentin ([2010](#_ENREF_32)) conducted a PMT-based study that concluded fear appeals influence users’ intentions to comply with individual acts of cybersecurity. In their study, perceptions of self-efficacy, response efficacy, threat severity, and social influence were found to inform the degree to which fear appeals impacted behavioral intentions. An organizational survey based on PMT used perceived severity, rewards, response efficacy, self-efficacy, and response costs to predict intentions to comply with IS security policies ([Vance et al., 2012](#_ENREF_61)). Another multi-organizational survey determined that perceived severity, response efficacy, self-efficacy, and response costs influence users’ attitudes toward cybersecurity policies ([Herath & Rao, 2009](#_ENREF_26)). A survey of college students showed that PMT is effective in increasing users’ willingness to use strong passwords ([Zhang & McDowell, 2009](#_ENREF_67)). A larger survey of non-students also demonstrated this tendency ([Milne et al., 2009](#_ENREF_44)). Finally, fear appeals have been shown to influence specific cybersecurity behaviors such as updating and protecting passwords ([Workman et al., 2008](#_ENREF_65)).

Our paper extends these findings to examine whether the use of just-in-time fear appeals, in response to the detection of password reuse, will discourage password reuse. In this paper, we explore using keystroke dynamics as a minimally invasive and low-cost method for identifying password reuse and triggering a just-in-time fear appeal – properties which make it a compelling solution for developing countries. *Keystroke dynamics* can be defined as behavioral characteristics of how a user types. In the seminal work by Gaines et al. ([1980](#_ENREF_20)), researchers collected precise measurements of keystroke timings and identified two attributes that are useful in developing a keystroke signature for a user: *dwell time*, or how long a key is held down, and *transition time*, or the latency between key presses. Based on this research, many studies have investigated using keystroke dynamics as a method to supplement the more traditional identification and authentication practice of using usernames and passwords ([Joyce & Gupta, 1990](#_ENREF_33); [Leggett & Williams, 1988](#_ENREF_36); [Park et al., 2010](#_ENREF_49); [Tappert et al., 2009](#_ENREF_59); [Teh et al., 2010](#_ENREF_60)).

Aside from an identification and authentication context, recent research in keystroke dynamics has demonstrated that typing characteristics may be linked to changes in cognitive load ([Vizer et al., 2009](#_ENREF_62)). Creating unique, strong passwords is a complex, mentally-taxing task that increases cognitive load ([Adams & Sasse, 1999](#_ENREF_1)) resulting in distinct cognitive processing compared to reusing routine passwords. We thus contend that monitoring changes in keystroke dynamics has potential for detecting password reuse. To date, however, researchers have yet to examine whether keystroke dynamics may be diagnostic of changes in cognitive processing and cognitive load associated with password reuse, and whether providing a just-in-time fear appeal will discourage password reuse when detected.

# Theory and Hypotheses

Integrating theories of routine, cognitive load, and motor movement, we first explain why users should exhibit different keystroke dynamics when creating a unique password as compared to typing routine information such as their name, email address, username, or a commonly used password. We then use PMT and theory on salience to explain why just-in-time fear appeals will decrease password reuse when violations are detected.

For typists, the cognitive nature of keystroke dynamics differs when typing routine words verses non-routine words (e.g., unique passwords). Routine words refer to strings that an individual has typed many times previously, such as their name, email address, and passwords that they frequently use. Theories explaining routine action ([e.g., Miller et al., 1986](#_ENREF_43)) posit that routine tasks are cognitively hierarchically structured indicating that higher-level goals initiate automatic lower-level tasks to fluently and rapidly coordinate behavior ([Shaffer, 1976](#_ENREF_54)). For example, when typists type routine words, they rarely think about the letters they are typing; instead, they think of the word, or collection of words, which activates the keystroke-execution processes for automatically typing each letter in the word ([Crump & Logan, 2010](#_ENREF_15)).

Logan and Crump explain this phenomenon as the inner–outer loop theory of typing ([Crump & Logan, 2010](#_ENREF_15); [Logan & Crump, 2009](#_ENREF_38)). This theory divides the cognitive process of typing into two separate hierarchical processes or ‘loops’—the outer loop and the inner loop. The outer loop transforms text or thoughts into a series of words and passes these words to the inner loop. The inner loop is an automatic and subconscious process that transforms each word into a series of coordinated hand and finger movements to make up the necessary keystrokes. The inner loop causes parallel activation of constituent keystrokes for each letter in the word and provides a serial control process ([John, 1996](#_ENREF_31); [Wu & Liu, 2008](#_ENREF_66)). According to this theory, the outer loop is unaware of the processes of the inner-loop. Because of this, typists typically have to think only of the word or sentence rather than thinking of the individual characters or the layout of the keyboard. Hence, typists have little explicit knowledge of what their fingers are doing ([Logan & Crump, 2009](#_ENREF_38)).

This hierarchical nature of typing has received considerable support in literature. For example, research has shown that the copy-typing rate is dependent on the word-like structure of the text. Words are typed much faster than random strings of characters, suggesting that words themselves play an important role in the cognitive processes that govern typing ([Crump & Logan, 2010](#_ENREF_15); [Larochelle, 1983](#_ENREF_35); [Shaffer & Hardwick, 1968](#_ENREF_55)). Typing speeds are also influenced by word-structure, such as syllable boundaries, indicating that word-level development is used during typing ([Weingarten et al., 2004](#_ENREF_63); [Will et al., 2006](#_ENREF_64)). Research has also shown that the mind processes the letters in the word or sentence congruently, and fingers move in parallel to type the words, as opposed to processing each letter individually ([Gentner et al., 1980](#_ENREF_22)). Finally, when typists are asked to recall the structure of a keyboard, type the letters for the left or right hand only, or pay attention to the keys that are being typed, typing performance decreases drastically. These results suggest that the word or sentence units activate subconscious lower-level processes that trigger the individual key strokes ([Logan, 2003](#_ENREF_37)).

When people type non-routine strings of characters, such as a strong unique password, typing is governed by different cognitive processes than when they are typing words or strings using the routine processes described previously. Creating a strong unique password requires significant cognitive attention ([Adams & Sasse, 1999](#_ENREF_1)). Strong passwords may be defined as non-routine words that include upper and lower-case letters, special characters, considerable length, and digits constructed in a manner such that the user can remember the password. The additional constraint of uniqueness requires the individual to create a password that has not been used before, further increasing cognitive load. During this cognitively demanding password composition process, typing flow is disturbed. Rather than relying on the outer-inner loop process to translate words into fluent and efficient keystroke behavior, the requirement to include special characters, digits, and upper or lower-case letters causes people to become conscious of what is being typed at the character level. Such behavior has been shown to significantly alter keystroke dynamics, typically by making it more sporadic and deliberate ([Crump & Logan, 2010](#_ENREF_15); [Larochelle, 1983](#_ENREF_35); [Shaffer & Hardwick, 1968](#_ENREF_55)).

In summary, we predict that keystroke dynamics will differ for individuals typing in routine information—such as a name, email address, or previously used passwords—versus individuals typing in non-routine information, as with a unique password. When users type in routine information, they will produce fluent, efficient, and consistent typing behavior that is governed by the outer-loop, inner-loop cognitive processing of words. However, when users create strong and unique passwords, their keystroke dynamics will be influenced by cognitive load and character-level cognitive processing. Accordingly, we propose the following hypothesis:

*H1. Creating strong unique passwords results in a measurable difference in keystroke dynamics as compared with typing known information*

When password reuse is detected through keystroke dynamics, the system can utilize just-in-time fear appeals to encourage users to create a unique password. To explain why fear appeals will decrease password reuse, we draw on PMT. PMT was originally constructed to help clarify how warnings, known as fear appeals, influence behavior ([Rogers, 1975](#_ENREF_51); [Rogers, 1983](#_ENREF_52)). Johnston and Warkentin ([2010](#_ENREF_32)) define a fear appeal as “…a persuasive message with the intent to motivate individuals to comply with a recommended course of action through the arousal of fear associated with a threat” (pp. 550-551). PMT explains that two appraisal processes take place when individuals are given a warning—a threat appraisal process and a coping appraisal process. The outcome of these two appraisal processes will determine whether the warning will be successful in changing behavior ([Rogers, 1983](#_ENREF_52); [Vance et al., 2012](#_ENREF_61)).

The threat appraisal process consists of assessing threat severity, threat vulnerability, and the benefit of behaving in a dangerous manner ([Rogers, 1983](#_ENREF_52)). In the context of password reuse, *severity* refers to the degree of hardship that can result from reusing a password. Passwords provide protection to many sensitive sites, including banks, email, social networking sites, and so on. Perceptions of severity include beliefs about the negative consequences that may result from being hacked due to password reuse on these sites, including identity theft, financial loss, personal data exposure, and loss of confidential information. The more severe one perceives the consequences of password reuse, the less likely it is that one will reuse passwords. *Vulnerability* refers to the probability that one will experience harm from reusing a password. Typically, people believe that only others with important information will be hacked, and thus they reuse passwords ([Zhang & McDowell, 2009](#_ENREF_67)). However, as one’s perception of vulnerability increases, password reuse should likewise decrease. Finally, *benefit* refers to the positive aspects of reusing passwords (e.g., easier to create and remember). If one perceives the benefit of reusing a password to be lower than the costs (e.g., the severity of and vulnerability to attack), they will likely not reuse passwords.

The coping-appraisal process consists of assessing response efficacy, self-efficacy, and response costs ([Rogers, 1975](#_ENREF_51)). In a password reuse context, *response efficacy* is the effectiveness of creating strong unique passwords to avoid being hacked or becoming a victim of a cybersecurity breach. People who believe that creating unique passwords reduces susceptibility are likely to avoid password reuse. *Self-efficacy* refers to one's personal belief in his/her ability to stop reusing passwords. Humans have cognitive limitations that deter them from making optimal security decisions. Working memory is limited, and therefore people must rely on strategies to remember unique passwords. The more a person believes that he or she has the ability and resources to not reuse a password, the more that individual will avoid password reuse. Finally, *response costs* refer to the costs of creating unique passwords. Response costs include the time and effort spent creating unique passwords, the cost of forgetting one’s password, the inconvenience of being locked out of a system, and so on. The frustration and inconvenience of forgetting a password is amplified by the large number of online accounts and passwords people have to remember. The higher one perceives the costs of creating unique passwords to be, the more likely one will reuse passwords ([Zhang & McDowell, 2009](#_ENREF_67)).

Fear appeals may inspire individuals to create strong and unique passwords through heightening perceptions of severity and vulnerability (the threat-appraisal process) as well as increasing perceptions of response efficacy and self-efficacy (the coping-appraisal process). Rogers ([1975](#_ENREF_51)) states,

“…a basic postulate is that protection motivation arises from the cognitive appraisal of a depicted event as noxious and likely to occur, along with the belief that a recommended coping response can effectively prevent the occurrence of the aversive event. If an event is not appraised as severe, as likely to occur, or if nothing can be done about the event, then no protection motivation would be aroused” (p. 99).

Just-in-time fear appeals should particularly have potential to heighten perceptions of severity, vulnerability, response efficacy, and self-efficacy because of the immediacy of the warning to the users’ behavior of creating a unique password. Immediacy has been shown to increase the salience of beliefs ([Crano, 1995](#_ENREF_13)). An individual’s working memory is limited, and information must compete for attention, therefore, only the most salient information will gain attention and influence behavior ([Miller, 1956](#_ENREF_42)). When creating a new user account, individuals may have several pieces of information competing for attention, including the primary purpose of creating an account, work responsibilities, time constraints, personal goals, and so forth ([Adams & Sasse, 1999](#_ENREF_1)). Given these other competing cognitions, severity, vulnerability, response efficacy, and self-efficacy may not be salient or “on the mind” of the user, and as such, the user may default to reusing a password. However, just-in-time warnings make perceptions of severity, vulnerability, response efficacy, and self-efficacy more salient, and thereby more likely to impact behavior. In summary, we propose:

*H2. Users who receive a just-in-time fear appeal discouraging password reuse are more likely to create unique passwords than users who do not receive a just-in-time fear appeal of password reuse*

# Methodology

To test our hypotheses, we conducted an experiment in which participants were required to create a user account on a website specially constructed for this study. After the first account creation screen, we randomly manipulated whether a just-in-time fear appeal was shown and, if so, gave the participant a second opportunity to create a unique password. We then compared whether users who received a just-in-time fear appeal created unique passwords more often than users who did not receive a just-in-time warning. During the account creation and login process, precise timing data for keystrokes was captured to build a model predicting password reuse.

## Participant Selection

A total of 148 students from a mid-level information systems course at a large public university in the Southwestern United States participated in the experiment. Participants were compensated with class credit for their participation. Client hardware and software configuration issues invalidated data from 13 of the participants, leaving usable data from 135 participants. Students were chosen for our sample because they commonly have multiple online accounts that may be targets for password reuse. The students represent an ethnically diverse population at this university, increasing the generalizability of this study to other nations and cultures. The average amount of college education was 3.2 years. Fifty-four percent of the participants were male and the average age was 23.4. The four most represented disciplines for the participants’ majors were Accounting (15%), MIS (15%), Marketing (13%), and Finance (11%). 55% of the participants were U.S. citizens, 16% Indian, 10% Mexican, 8% Chinese, and 11% citizens of other countries.

## Experiment Task and Procedure

To participate in the experiment, all participants were required to create a user account and password on a registration system specially crafted for the experiment (Figure 1). During the account creation process, participants provided several pieces of routine information, specifically their name, university email address, and preferred username. The account creation process also required users to provide a password, which they self-selected to create uniquely or to reuse an existing password. Precise keystroke timing information was collected for each field, which was later used to establish a baseline of keystroke dynamics characteristics. Note that to protect the privacy of participants, only statistical properties of keystroke dynamics were recorded and this information was decoupled from personal identifiers.

|  |
| --- |
|  |
| Figure 1. Account creation page |

After entering the required information and clicking the “Create Account” button, participants were assigned randomly to a “warning treatment” (n=69) or a “non-warning treatment” (n=66). If assigned to the warning treatment, they were shown the prompt in Figure 2.

|  |
| --- |
| We have detected that you may have used this password on other websites. Using the same password for multiple sites puts you at high risk of being hacked. To protect your privacy, **please choose a unique password for this website.** |
| Figure 2. Fear appeal text |

Participants were then prompted to re-enter the same information needed to create an account, including a password. Participants were not prohibited from entering the same password that they previously used. The fear appeal message was specifically crafted to leverage principles from PMT to persuade the participant to create a unique password. The term “high risk” was included to increase the perceived vulnerability and the term “hacked” was included to increase perceived severity of reusing a password. The last sentence in the prompt explains how to protect against hackers by creating a unique password, thus increasing efficacy. After completing the account creation process successfully, users in both conditions were presented with a login screen where they were prompted to provide the username and password they had just created to access the system. After participants logged in, they were presented with a brief survey as described below.

## Survey Instruments

In a post-experiment survey, PMT constructs—perceived severity, perceived vulnerability, response efficacy, and self-efficacy adapted from Vance et al. ([2012](#_ENREF_61)) were captured as a manipulation check. Participants were then asked if they created a unique password when they first attempted to create an account (Figure 3). Finally, for participants who received the fear appeal treatment, the survey asked if they created a unique password on their second attempt (Figure 4).

|  |
| --- |
| When you FIRST created a password on the account creation page, did you use a password that you have ever used before (e.g., your email password, school password, bank, iTunes, computer password, etc.)?  PLEASE ANSWER THIS QUESTION TRUTHFULLY. We are conducting a study about password reuse behaviour. Your privacy is protected, and your password will not be saved.  ○ I used a password I have used before when I FIRST created a password in this experiment  ○ I created a unique password when I FIRST created a password in this experiment |
| Figure 3. Password reuse question   |  | | --- | | After being prompted to create a unique password, did you create a unique password (e.g., a password you have never used before on any account)?  ○ Yes  ○ No |   Figure 4: Password reuse question after fear appeal | | |

## Keystroke Dynamics

To predict password reuse, we captured characteristics of participants’ typing patterns for analysis. A JavaScript application was created to record key codes and the time (in milliseconds) at which each key was pressed and released. This code was embedded into the account creation and login pages of the experiment web site. Statistical data collected by the application were stored in a SQL database.

After data collection, algorithms were used to transform the raw keystroke timing data into digraph patterns and to calculate dwell time, transition time, and typing speed for each element that was entered (name, email address, username, password, and password confirmation). *Dwell times* were calculated by subtracting the time that each key was pressed from the time it was released. *Transition times* were calculated by subtracting the time a key was released from the time the subsequent key was pressed. Approximately 80% of the transition and dwell times were used in the subsequent analysis. The remaining 20% of individuals’ transition and dwell times were not used because they contained substantial corrections which invalidated the keystroke data (i.e. dozens of corrections or holding down keys for extended periods of time), invalid characters (a bi-product of some browsers and operating systems), or long pauses outside 3 standard deviations of the average. Typing speed was then calculated by dividing the total number of milliseconds each field took to type by the number of characters entered into the field, then dividing the result by 1000, resulting in a measure of characters per second.

# Data Analysis and Results

Prior to the full data analysis, we assessed the validity and reliability of the adapted measures. Convergent and discriminant validity of measurement scales were assessed through a factor analysis using Varimax rotation as well as construct correlations and cross-correlations. All of the loadings of each item on its latent construct exceeded 0.6 and loaded less than 0.35 on other constructs. Average variance extracted (AVE) of all constructs was much larger than 0.5, therefore good convergent validity was demonstrated ([Anderson & Gerbing, 1988](#_ENREF_2)). Additionally, all square roots of AVE exceeded the correlation coefficients between constructs and therefore demonstrated good discriminant validity ([Fornell & Larcker, 1981](#_ENREF_18)). Finally, all Cronbach's alpha scores were above the 0.7 score suggested by Nunnally ([1978](#_ENREF_46)).

To ensure that the fear appeals presented to participants elicited the desired effects based on PMT, we then conducted manipulation checks on perceived severity, vulnerability, response efficacy, and self-efficacy with an ANOVA. The manipulation checks supported that the fear appeals influenced perceptions of severity (*F (*df = 133) = 12.123, *p* = .001), vulnerability (*F (*df = 133) = 4.227, *p* = .043), and response efficacy (*F (*df = 133) = 9.131, *p* = .003). The manipulation did not influence self-efficacy significantly (*F (*df = 133) = 1.860, *p* = .176), possibly because we did not provide training on strategies for composing unique passwords.

## Hypothesis Testing

### Hypothesis 1

To test hypothesis 1— *creating strong unique passwords results in a measurable difference in keystroke dynamics as compared with typing known information*—we evaluated our data using both statistical analysis of keystroke dynamics and a support vector machine (SVM) in WEKA, a popular suite of machine learning software ([Hall et al., 2009](#_ENREF_25)).

In our initial analysis of the data, we calculated the average transition time and dwell time for the three non-password fields together along with the averages, standard deviations, and z-scores for each of the five fields individually for all users. Deviations in transition time and dwell time were used to generate features to classify password reuse. In the first row in Table 2, we show transition data from the first account creation screen for users who indicated they reused a password. The data indicate that users typically type their name and email address slightly slower than average (11% and 9% respectively), and type their username approximately 26% faster than the average of all non-password fields. The password and password confirmation fields are 35-36% slower than non-password fields. Fifty-three participants in the fear appeals condition reported reusing a password initially, but creating a unique password after being prompted. We conducted a within-subject t-test to examine whether participants’ keystroke dynamics were statistically different when creating unique passwords compared to reusing passwords. After receiving the prompt to create a new unique password and again filling out the fields on the account creation page, our results indicate no statistically significant difference in keystroke dynamics for name (*t(*df = 52) = -0.523, *p* =.603), email address (*t(*df = 52) = -0.429, *p* =.670), or username (*t(*df = 52) = -0.811, *p* =.421) for these participants, however, the speed with which the password is typed drops dramatically from an average of 81ms between key presses to an average of 107ms as shown in Table 2. This within-subject difference between typing non-unique passwords (first attempt) and typing unique passwords (second attempt) is highly significant (*t (*df = 52) = - 3.448, *p* =.001). Thus, H1 was supported

Table 2: Analysis of transition times

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | Average transition time (ms) | Name (ms) and % of average | Email Address (ms) and % of average | Username (ms) and % of average | Password (ms) and % of average | Password  Confirmation (ms) and % of average |
| First Attempt  (Non-unique password) | 59 | 66 (111%) | 65  (109%) | 44  (74%) | 81  (136%) | 80  (135%) |
| Second Attempt  (Unique Password) | 60 | 65  (109%) | 61  (103%) | 40  (67%) | 111  (186%) | 103  (172%) |

In a supplemental analysis, we build on this initial extraction and analysis of transition time and dwell time features to create a classification algorithm for identifying non-unique passwords using a support vector machine in WEKA. A support vector machine is a supervised learning approach that constructs a set of hyperplanes in a high-dimensional space. It uses a linear model to implement nonlinear class boundaries through mapping input vectors into the high-dimensional feature space. In this feature space, an optimal separating hyperplane is constructed. This hyperplane gives the maximum separation between decision classes. The training examples that are closest to the maximum margin hyperplane are called support vectors ([Cristianini & Shawe-Taylor, 2000](#_ENREF_14)).

Before applying the support vector machine learning approach, we performed feature selection using Classifier Subset Evaluator for WEKA’s support vector machine implementation—SMO. We used a best first search method to select features based on the raw values, averages, standard deviations, and z-scores of transition time and dwell time for each field. After selecting the attributes, we created a classification model by applying WEKA’s SMO classifier to the data. The results were validated using 10-fold cross validation, and are shown in Table 3.

Table 3: Support vector machine classification results

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Class | True Positive Rate1 | False Positive Rate2 | Precision3 | Recall4 | F-Measure5 |
| Created Unique Password | 0.811 | 0.178 | 0.789 | 0.811 | 0.800 |
| Reused Password | 0.822 | 0.189 | 0.841 | 0.822 | 0.831 |
| 1. The fraction of users correctly classified as a hit (i.e., as creating a unique password or reusing a password) 2. The fraction of users incorrectly classified as a hit 3. The fraction of instances classified as a hit that are actually a hit 4. The fraction of hits that are classified as a hit. 5. The harmonic mean of precision and recall (a combined statistic of precision and recall) | | | | | |

### In summary, we were able to successfully distinguish between users who created unique passwords and users who reused passwords based on keystroke dynamics. Our model correctly classified 81.71% of participants.

### Hypothesis 2

To test hypothesis 2—*users who receive a just-in-time fear appeal deterring password reuse are more likely to create unique passwords than users who do not receive a just-in-time fear appeal of password reuse*—we performed a between-subjects *t*-test comparing the percentage of people who created unique passwords in the non-fear appeal group to the percentage of people who created unique password in the fear appeal group. This test was performed using the “two sample *t*-test between percents” from the StatPac Statistics Calculator. Table 4 summarizes the percentages of unique passwords in each group. The difference between the two groups was highly significant (*t (*df = 133) = 7.874, *p* < .001); hence, H2 was supported.

Table 4. Summary of unique passwords in manipulations

|  |  |  |  |
| --- | --- | --- | --- |
| Received fear appeal | # of participants | # of participants who created a unique password | % of participants who created unique passwords |
| No | 66 | 3 | 4.45% |
| Yes | 69 | 61 | 88.41% |

# Discussion

This article addressed two research questions. The first research question asked whether keystroke dynamics could be used to predict if people are reusing passwords. To answer this research question, we monitored keystroke dynamics—specifically transition time and dwell time—on the account creation page of a web site. We found significant differences in transition times between unique and non-unique passwords. We also trained a support vector machine and were able to correctly classify password reuse with an overall accuracy rate of 81.71%. Hence, we conclude that H1 was supported and that it is possible to detect password reuse by monitoring users’ keystroke dynamics.

Our second research question asked whether providing just-in-time fear appeals would help reduce password reuse. In our study, approximately half of the participants were given a just-in-time fear appeal discouraging them from reusing passwords. The fear appeal was created based on constructs found in PMT, and significantly influenced perceptions of threat severity, threat vulnerability, and response efficacy. After receiving the fear appeal, 88.41% of participants created unique passwords. Conversely, in the group that did not received the fear appeal, only 4.45% of participants created unique passwords. The difference between the two groups was highly significant, supporting H2. We conclude that just-in-time fear appeals decrease password reuse.

# Implications for Research

This paper makes several important contributions to research. First, our research highlights the need to understand and mitigate password reuse. In our data collection, only 7 out of 135 participants (5.19%) created a unique password during their first interaction with our system. This illustrates the prevalence of password reuse. Few extant studies have examined how to alleviate password reuse, especially in situations where users may have little or no opportunity for formal cybersecurity education and shared computer use is high—as is the case in developing countries. Our research helps address this need by explaining how keystroke dynamics can be diagnostic of password reuse and how just-in-time fear appeals can decrease password reuse all within the account creation page of a web site.

To our knowledge, this is the first study to examine how keystroke dynamics can be used to identify password reuse. Although considerable research has been conducted with regard to keystroke dynamics as a supplement to traditional authentication mechanisms, existing research examining changes in keystroke dynamics as a proxy for cognitive changes is scarce. In our study, we show that changes in keystroke dynamics are indicative of password reuse, and theoretically explain why differences in keystroke dynamics may result from changes in a user’s cognitive processing and level of cognitive load. Building on this theory, we were able to construct an algorithm for identifying password reuse with an accuracy rate of 81.71%. Future research should examine whether other forms of insecure behaviour can be detected through changes in keystroke dynamics.

Finally, we contribute to theory by extending PMT to the context of password reuse. We found that just-in-time fear appeals to avoid password reuse promote unique password creation. We theorize that this effect is due to the increased salience of the message due to the immediacy of the fear appeal. Rarely is the act of ‘being secure’ the primary purpose of using a computer; rather, computers are used to achieve other goals such as increasing productivity, communicating, socializing, entertainment, and more. These other goals compete for the user’s attention, and cybersecurity beliefs, such as the severity and vulnerability of a threat, are often overcome by these other motives. Just-in-time fear appeals may make cybersecurity beliefs, such as those found in PMT, more salient, thereby decreasing password reuse.

# Implications for Practice

Password reuse is pervasive. Even the most technically-sound system can be breached by stolen credentials when individuals reuse passwords across multiple accounts. The detrimental effects of password reuse are particularly difficult to combat in developing countries where systems may lack adequate cybersecurity controls, individuals often use public computers which limit the applicability of password management systems, government programs may not be in place to enforce cybersecurity laws, and public cybersecurity education is either scarce or non-existent. To protect individuals against password reuse, this article proposes a cost-effective method to deter password reuse. The tool focuses on changing users’ password creation behaviour through two components. First, the system detects when password reuse is present. The prediction algorithm monitors keystroke dynamics characteristics on account creation pages to detect possible password reuse. When password reuse is detected, we found that a simple just-in-time fear appeal can be used to change users’ password creation behaviour, increasing the use of unique passwords in this study from 4.45%, when no fear appeal is used, to 88.41% when a just-in-time fear appeal is presented.

# Limitations and Future Research

Future research should examine how just-in-time fear appeals influence user satisfaction, especially for users who are falsely accused (false-positives). Because of the small percentage of participants who created unique passwords prior to receiving the fear appeal in our study (7 out of 135, only 3 of which were in the fear appeal condition), we did not have adequate statistical power to compare the satisfaction of users who unjustly received the fear appeal and people who rightfully received the fear appeal. Based on expectation-confirmation theory ([Oliver, 1977](#_ENREF_48)), we predict that users who unjustly receive the fear appeal will experience a decrease in satisfaction with the system. Expectation-confirmation theory explains that confirming or disconfirming an individual’s expectations will influence satisfaction. If perceived performance of the system falls short of an individual’s expectations, this negative disconfirmation will decrease satisfaction. Ultimately, the level of satisfaction or dissatisfaction experienced by the user will influence their tendency to use, repurchase, return, or discontinue the use of a product or service ([Lowry et al., 2009](#_ENREF_39); [McKinney et al., 2002](#_ENREF_41)). We predict that users who unjustly receive a fear appeal to create a unique password will experience a negative disconfirmation and view the website as less usable, which will result in a decrease in satisfaction. Future research should validate this proposition.

Future research should also seek to improve the classification accuracy of password reuse. Although 81.71% is promising, we believe significant improvement can be made. One possible feature to further improve the algorithm’s accuracy is through more sophisticated keystroke dynamics analysis, in which digraph patterns for unique and non-unique password are compared against larger sets of routine and non-routine text. This approach would require the collection of significantly more text than is typically available during the account creation process, but could be easily incorporated into other studies using keystroke dynamics.

Furthermore, future research should cross-validate the results of this study in a developing country. Our student-based sample consists of individuals who are largely computer literate and mostly competent typists, which may limit the generalizability of our findings. Typing fluency may vary across different samples especially in developing countries, which may influence the features that predict password reuse. However, research has suggested that despite potential large differences between users (e.g., in terms of typing fluency, computer skills, language etc.), the keystroke dynamic differences within users will likely be constant ([Gunetti & Picardi, 2005](#_ENREF_23); [Gunetti et al., 2005](#_ENREF_24)). Future research should validate the generalizability of our findings, and identify which features are most diagnostic in various populations.

Finally, our research only examined whether users’ passwords were unique. We did not examine the overall strength of the password, nor did we investigate the pros and cons of different password creation strategies. It is possible that having more controls (e.g., requiring users to create unique passwords) can cause users to create passwords with lower password entropy as a negative side effect ([Jenkins et al., 2010](#_ENREF_30)). Thus, future research should more comprehensively examine how extensively password reuse should be discouraged (i.e. for all accounts or only for highly sensitive accounts) and how prompting users to create unique password may influence the entropy of passwords they create. Furthermore, future research should investigate how different password-creation strategies can encourage both password strength and uniqueness.

# Conclusion

This paper helps address the need to reduce password reuse. Password reuse presents a security risk as a single stolen password can be used to gain unauthorized access a wide range of important websites and systems. In this study, we theoretically explain why password reuse can be detected through monitoring keystroke dynamics on account creation pages. We also proposed that providing just-in-time fear appeals when violations are detected will decrease password reuse by making important cybersecurity beliefs more salient. We tested our hypotheses experimentally and found that keystroke dynamics are diagnostic of password reuse. Keystroke dynamics of users who created unique passwords were significantly different than the keystroke dynamics of users who reused passwords. Using this knowledge, we created a support vector machine capable of identifying password reuse with 81.71% accuracy. We also found that just-in-time fear appeals strongly decreased password reuse; 88.41% of people who received a just-in-time fear appeal created unique passwords whereas only 4.45% of people who did not receive a fear appeal created a unique password. This paper demonstrates that keystroke dynamics can be used to assess complex human behaviour and cognitive processing, and that just-in-time fear appeals are a highly influential and cost-effective way to decrease password reuse. Developing countries may be able to realize gains in information systems cybersecurity by leveraging the minimally-invasive and cost-effective methods described in this paper.

# References

Adams, A., & Sasse, M. A. (1999). Users are not the enemy. *Communications of the ACM, 42*(12), 40-46.

Anderson, J. C., & Gerbing, D. W. (1988). Structural equation modeling in practice: A review and recommended two-step approach. *Psychological Bulletin, 103*(3), 411-423.

Biddle, R., Chiasson, S., & Van Orschot, P. C. (2012). Graphical passwords: Learning from the first twelve years. *ACM Computing Surveys, 44*(4), 19:11-19:41.

Bonneau, J., Herley, C., van Oorschot, P. C., & Stajano, F. (2012, May 20-23). *The quest to replace passwords: A framework for comparative evaluation of web authentication schemes.* Paper presented at the 2012 IEEE Symposium on Security and Privacy, San Francisco, CA.

Brechbuhl, H., Bruce, R., Dynes, S., & Johnson, M. E. (2010). Protecting critical information infrastructure: Developing cybersecurity policy. *Information Technology for Development, 16*(1), 83-91.

Bryant, K., & Campbell, J. (2006). User behaviours associated with password security and management. *Australasian Journal of Information Systems, 14*(1), 81-100.

Campbell, J., Kleeman, D., & Ma, W. (2007). The good and not so good of enforcing password composition rules. *Information Systems Security, 16*(1), 2-8.

Campbell, J., Ma, W., & Kleeman, D. (2011). Impact of restrictive composition policy on user password choices. *Behaviour & Information Technology, 30*(3), 379-388.

Carte, T. A., Dharmasiri, A., & Perera, T. (2011). Building IT capabilities: Learning by doing. *Information Technology for Development, 17*(4), 289-305.

Charoen, D., Murali, R., & Lorne, O. (2008). Improving end user behaviour in password utilization: An action research initiative. *Systemic Practice & Action Research, 21*(1), 55-72.

Chen, Y. N., Chen, H. M., Huang, W., & Ching, R. K. H. (2006). E-government strategies in developed and developing countries: An implementation framework and case study. *Journal of Global Information Management, 14*(1), 23-46.

Cone, B. D., Irvine, C. E., Thompson, M. F., & Nguyen, T. D. (2007). A video game for cyber security training and awareness. *Computers & Security, 26*(1), 63-72.

Crano, W. D. (1995). Attitude strength and vested interest. In R. E. Petty & J. A. Krosnick (Eds.), *Attitude Strength: Antecedents and Consequences* (pp. 131–158). Mahwah, NJ, USA: Erlbaum.

Cristianini, N., & Shawe-Taylor, J. (2000). *An Introduction to Support Vector Machines And Other Kernel-Based Learning Methods*. Cambridge, UK: Cambridge University Press.

Crump, M. J. C., & Logan, G. D. (2010). Hierarchical control and skilled typing: Evidence for word-level control over the execution of individual keystrokes. *Journal of Experimental Psychology-Learning Memory and Cognition, 36*(6), 1369-1380.

Florencio, D., & Herley, C. (2006, July 12-14). *How to login from an internet cafe without worrying about keyloggers.* Paper presented at the Symposium on Usable Privacy and Security, Pittsburgh, PA.

Florencio, D., & Herley, C. (2007, May 08-12). *A large-scale study of web password habits.* Paper presented at the 16th international conference on World Wide Web, Banff, Alberta, Canada.

Fornell, C., & Larcker, D. F. (1981). Evaluating structural equation models with unobservable variables and measurement error. *Journal of Marketing Research, 18*(1), 39-50.

Furnell, S. (2007). An assessment of website password practices. *Computers & Security, 26*(7-8), 445-451.

Gaines, R. S., Lisowski, W., Press, S. J., & Shapiro, N. (1980). Authentication by keystroke timing: Some preliminary results: RAND Corporation.

Gaw, S., & Felten, E. W. (2006, July 12-14). *Password management strategies for online accounts.* Paper presented at the Second Symposium on Usable Privacy and Security, Pittsburgh, PA, USA.

Gentner, D. R., Grudin, J., & Conway, E. (1980). *Finger movements in transcription typing*. San Diego: University of California at San Diego, Center for Human Information Processing.

Gunetti, D., & Picardi, C. (2005). Keystroke analysis of free text. *ACM Transactions on Information and System Security (TISSEC), 8*(3), 312-347.

Gunetti, D., Picardi, C., & Ruffo, G. (2005). Keystroke analysis of different languages: A case study. *Advances in Intelligent Data Analysis, 6*(1), 133-144.

Hall, M., Frank, E., Holmes, G., Pfahringer, B., Reutemann, P., & Witten, I. H. (2009). The WEKA Data Mining Software: An Update. *SIGKDD Explorations, 11*(1), 10-18.

Herath, T., & Rao, H. R. (2009). Protection motivation and deterrence: A framework for security policy compliance in organisations. *European Journal of Information Systems, 18*(2), 106-125.

Huang, C.-Y., Ma, S.-P., & Chen, K.-T. (2011). Using one-time passwords to prevent password phishing attacks. *Journal of Network & Computer Applications, 34*(4), 1292-1301.

Hwang, M.-S., Chong, S.-K., & Chen, T.-Y. (2010). DoS-resistant ID-based password authentication scheme using smart cards. *Journal of Systems & Software, 83*(1), 163-172.

Ives, B., Walsh, K. R., & Schneider, H. (2004). The domino effect of password reuse. *Communications of the ACM, 47*(4), 75-78.

Jenkins, J. L., Durcikova, A., Ross, G., & Nunamaker Jr, J. F. (2010, December 12-15). *Encouraging users to behave securely: Examining the influence of technical, managerial, and educational controls on users’ secure behavior.* Paper presented at the International Conference on Information Systems, Saint Louis, Missouri.

John, B. E. (1996). TYPIST: A theory of performance in skilled typing. *Human-Computer Interaction, 11*(4), 321-355.

Johnston, A. C., & Warkentin, M. (2010). Fear appeals and information security behaviors: An empirical study. *MIS Quarterly, 34*(3), 549-565.

Joyce, R., & Gupta, G. (1990). Identity authentication based on keystroke latencies. *Communications of the ACM, 33*(2), 168-176.

Keith, M., Shao, B., & Steinbart, P. (2009). A behavioral analysis of passphrase design and effectiveness. *Journal of the Association for Information Systems, 10*(2), 63-89.

Larochelle, S. (1983). A comparison of skilled and novice performance in discontinuous typing. In W. E. Cooper (Ed.), *Cognitive Aspects of Skilled Typewriting* (pp. 67–94). New York, NY, USA: Springer-Verlag.

Leggett, J., & Williams, G. (1988). Verifying identity via keystroke characteristics. *International Journal of Man-Machine Studies, 28*(1), 67-76.

Logan, G. D. (2003). Simon-type effects: Chronometric evidence for keypress schemata in typewriting. *Journal of Experimental Psychology-Human Perception and Performance, 29*(4), 741-757.

Logan, G. D., & Crump, M. J. C. (2009). The left hand doesn’t know what the right hand is doing: The disruptive effects of attention to the hands in skilled typewriting. *Psychological Science, 10*(1), 1296–1300.

Lowry, P. B., Romano, N. C., Jenkins, J. L., & Guthrie, R. W. (2009). The CMC interactivity model: How interactivity enhances communication quality and process satisfaction in lean-media groups. *Journal of Management Information Systems, 26*(1), 155-195.

Maurer, T. (2011). Cyber norm emergence at the United Nations—an analysis of the UN’s activities regarding cyber-security *Explorations in Cyber International Relations Discussion Paper Series*: Belfer Center for Science and International Affairs, Harvard Kennedy School.

McKinney, V., Yoon, K., & Zahedi, F. (2002). The measurement of web-customer satisfaction: An expectation and disconfirmation approach. *Information Systems Research, 13*(3), 296-315.

Miller, G. A. (1956). The magical number seven plus or minus two: Some limits on our capacity for processing information. *Psychological Review, 63*(2), 81-97.

Miller, G. A., Galanter, E., & Pribram, K. H. (1986). *Plans and the Structure of Behavior*. New York, NY, USA: Adams-Bannister-Cox.

Milne, G. R., Labrecque, L. I., & Cromer, C. (2009). Toward an understanding of the online consumer's risky behavior and protection practices. *Journal of Consumer Affairs, 43*(3), 449-473.

Notoatmodjo, G., & Thomborson, C. (2009, January 20-21). *Passwords and perceptions.* Paper presented at the Seventh Australasian Conference on Information Security, Wellington, New Zealand.

Nunnally, J. C. (1978). *Psychometric Theory* (2nd ed.). New York, NY, USA: McGraw-Hill.

Oghenerukevbe, E. A. (2010). Mnemonic passwords practices in corporate sites in Nigerian. *Journal of Internet Banking & Commerce, 15*(1), 1-11.

Oliver, R. L. (1977). Effect of expectation and disconfirmation on postexposure product evaluations - Alternative interpretation. *Journal of Applied Psychology, 62*(4), 480-486.

Park, S., Park, J., & Cho, S. (2010, June 29-July 1). *User authentication based on keystroke analysis of long free texts with a reduced number of features.* Paper presented at the 2010 Second International Conference on Communication Systems, Networks and Applications (ICCSNA), Hong Kong, China.

Pick, J. B., & Azari, R. (2008). Global digital divide: Influence of socioeconomic, governmental, and accessibility factors on information technology. *Information Technology for Development, 14*(2), 91-115.

Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change. *Journal of Psychology, 91*(1), 93-114.

Rogers, R. W. (1983). Cognitive and physiological processes in fear appeals and attitude change: A Revised theory of protection motivation. In J. Cacioppo & R. Petty (Eds.), *Social Psychophysiology* (pp. 153-176). New York, NY, USA: Guilford Press.

Roztocki, N., & Weistroffer, H. R. (2011). Information technology success factors and models in developing and emerging economies. *Information Technology for Development, 17*(3), 163-167.

Shaffer, L. H. (1976). Intention and performance. *Psychological Review, 83*(5), 375-393.

Shaffer, L. H., & Hardwick, J. (1968). Typing performance as a function of text. *Quarterly Journal of Experimental Psychology, 20*(4), 360-369.

Shouhong, W., & Hai, W. (2008). Password authentication using Hopfield neural networks. *IEEE Transactions on Systems, Man & Cybernetics: Part C - Applications & Reviews, 38*(2), 265-268.

Tagert, A. C. (2010). *Cybersecurity Challenges in Developing Nations.* Doctor of Philosophy, Carnegi Mellon University, Pittsburgh, PA.

Tam, L., Glassman, M., & Vandenwauver, M. (2010). The psychology of password management: A tradeoff between security and convenience. *Behaviour & Information Technology, 29*(3), 233-244.

Tappert, C., Villani, M., & Cha, S.-H. (2009). Keystroke biometric identification and authentication on long-text input. In L. Wang & X. Geng (Eds.), *Behavioral Biometrics for Human Identification: Intelligent Applications* (pp. 342-367). Hershey, PA: IGI Global.

Teh, P. S., Teoh, A. B. J., Tee, C., & Ong, T. S. (2010). Keystroke dynamics in password authentication enhancement. *Expert Systems with Applications, 37*(12), 8618-8627.

Vance, A., Siponen, M., & Pahnila, S. (2012). Motivating IS security compliance: Insights from habit and protection motivation theory. *Information & Management, 49*(3-4), 190-198.

Vizer, L. M., Zhou, L. N., & Sears, A. (2009). Automated stress detection using keystroke and linguistic features: An exploratory study. *International Journal of Human-Computer Studies, 67*(10), 870-886.

Weingarten, R., Nottbusch, G., & Will, U. (2004). Morphemes, syllables, and graphemes in written word production. In T. Pechmann & C. Habel (Eds.), *Language Production* (pp. 529–572). Berlin, Germany: Mouton de Gruyter.

Will, U., Nottbusch, G., & Weingarten, R. (2006). Linguistic units in word typing: Effects of word presentation modes and typing delay. *Written Language & Literacy, 9*(1), 153-176.

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

Wu, C., & Liu, Y. (2008). Queuing network modeling of transcription typing. *ACM Transactions on Computer-Human Interaction, 15*(1).

Zhang, L., & McDowell, W. C. (2009). Am I really at risk? Determinants of online users' intentions to use strong passwords. *Journal of Internet Commerce, 8*(3/4), 180-197.

1. *Cybersecurity* is used to refer to the body of practices, technologies, and processes designed to protect cyber-infrastructure (e.g., data, networks, computers, software) and user assets from attack, damage, and unauthorized access and use ([Brechbuhl et al., 2010](#_ENREF_5)) [↑](#footnote-ref-1)