Exploring how Dual-Task Interference Influences End-User Secure Behavior

Work-In-Progress

Jeffrey L. Jenkins
Brigham Young University
Provo, UT
jjenkins@byu.edu

Alexandra Durcikova
University of Oklahoma
Norman, Oklahoma
alex@ou.edu

K. Shane Reeves
Brigham Young University
Provo, UT
kshanereeves@byu.edu

ABSTRACT

People use computers for a myriad of purposes, including to accomplish work-related tasks, entertainment, and communication. At the same time, users must inadvertently interact with security mechanisms and make security decisions. Humans, however, normally have trouble performing two or more relatively simple tasks concurrently—a phenomenon known as dual-task interference. This research-in-progress article explores how dual-task interference influences users’ secure behavior (i.e., compliance with organizational security policies and best practices). The article hypothesizes how dual-task interference may influence two types of common security activities: a) security activities that are performed simultaneously with other activities (e.g., assessing the credibility of sources while reading emails or browsing the web), and b) security activities that interrupt users’ other activities to request a security action (e.g., warnings or prompts). The article proposes two experiments to test the hypotheses about how dual-task interference influences these two types of security activities. At the time of this submission, pilot tests were underway to further refine the experimental designs. Pending on whether the hypotheses are supported, this research highlights the need for conducting future research that focuses on alleviating the effects of dual-task interference (a physiological limitation of humans) in addition to the existing approaches on exploring how to improve users’ security beliefs and intentions.

KEYWORDS

Dual task interference, secure behavior, phishing, passwords, simultaneous security behaviors, discrete security behaviors.
EXPLORING HOW DUAL-TASK INTERFERENCE INFLUENCES END-USER SECURE BEHAVIOR

Work-In-Progress

INTRODUCTION

Identifying sources of non-compliance with an organization’s security policies has important theoretical and practical implications. By understanding ‘why’ employees disobey security policies, researchers can endeavor to discover and apply theories that explain how to alleviate the source of non-compliance. Practitioners can then implement interventions to promote secure behavior based on this research. For example, security research has identified inadequate training as a source of non-secure behavior (i.e., non-compliance with security policy) and has thereby sought to understand how to create better security education, training, and awareness (SETA) programs (e.g., D'Arcy et al. 2009; Puhakainen and Siponen 2010). As a result, interventions have been suggested to improve the effectiveness of training programs, including the use of online training videos (Furnell et al. 2002; Workman and Gatheygi 2007), face-to-face discussions (Hollinger and Clark 1983), checklists, web-based tutorials (Cox et al. 2001), verbal persuasion, vicarious experience (Warkentin et al. 2011), and mock exercises (Dodge et al. 2007), to name a few. However, in spite of these efforts (and others), employees’ non-compliance with security policy has not completely diminished (Schneier 2005), suggesting the need to explore other reasons for non-compliance.

This research-in-progress explores another potential source of non-compliance: dual-task interference. Dual-task interference is a phenomenon that explains why people have trouble performing two or more relatively simple tasks concurrently (Pashler 1994). Normally, people are not aware of tasks interfering with each other unless they are cognitively difficult or physically incompatible (e.g., talking on a cell phone while driving). Hence, it might seem that only exceptional activities suffer from dual-task interference. Studies, however, demonstrate that just the
opposite case is true (Borst et al. 2012; Fougnie and Marois 2009; Hiraga et al. 2009; Pashler 1990; Pashler 1994; Pashler et al. 1993; Pearson and Sawyer 2011; Telford 1931); tasks can “interfere with each other quite drastically, even though they are neither intellectually challenging nor physically incompatible” (Pashler 1994 p. 220).

Dual-task interference may be particularly useful for understanding users’ compliance with organizational security policies and best practices (which we refer to as secure behavior in this paper), because the act of behaving securely is rarely the primary purpose of using a computer (West 2008). Rather, users primarily use a computer to accomplish other tasks such as communicating with other people or performing work-related tasks. As a bi-product of performing these other tasks, users unavoidably encounter security threats (e.g., phishing emails, potentially harmful websites, etc.) or security prompts (a prompt to create a password, login to a system, or verify an identity) (Adams and Sasse 1999; Forget et al. 2007; West 2008). As these security encounters often occur at the same time as performing the other primary tasks, they are prime targets of dual-task interference (Pashler 1994).

The purpose of this research is to explore how dual-task interference influences secure behavior. The article first briefly summarizes relevant literature on dual-task interference. Second, it theorizes why dual-task interference may decrease secure behavior. The article then proposes a set of experiments. The first experiment explores how dual-task interference influence secure behavior while performing security tasks simultaneously with other tasks. The second experiment explores how dual-task interferences influences secure behavior when other tasks are interrupted to perform security tasks (e.g., when a system prompts a user to perform a security action). Finally, the article explores the theoretical and practice contributions of understanding how dual-task interference influences end-user secure behaviors. Namely, this article helps establish an innovative area of end-user security research— theoretically and empirically understanding how to alleviate the influence of dual-task interference on secure behavior.
LITERATURE REVIEW

Dual-task interference has been shown to decrease performance in a wide variety of tasks (Pashler 1994). For example, the news is frequented by reports of automobile accidents resulting from a person trying to drive and talk on a cellphone at the same time. Indeed, research has verified that activities such as driving and talking on a cell phone result in dual-task interference which may decrease performance in one or both of the activities (Strayer and Johnston 2001). However, research has also verified that performing multiple relatively simple or insignificant tasks at the same time may also result in dual-task interference and decrease performance (Borst et al. 2012; Fougnie and Marois 2009; Hiraga et al. 2009; Pashler 1990; Pashler 1994; Pashler et al. 1993; Pearson and Sawyer 2011; Telford 1931). For example, concurrent processing may decrease users’ performance in simple visual search and dichotic monitoring tasks (Duncan and Coltheart 1987; Kleiss and Lane 1986). When asked to count at the same time as recognizing stimuli, people cannot find alternative organizations of ambiguous stimuli as quickly (Reisberg 1983). When consuming people’s short term memory by asking them to memorize a simple piece of information for later recall, the speed at which people can perform other tasks decreases (Logan 1978). In more recent examples, research has found that dual-task interference for some tasks results from competition for the same brain areas / functions (Rémy et al. 2010), and dual-task interference increases when performing two or more tasks simultaneously while experiencing stress (Plessow et al. 2012).

In an information systems context, dual-task interference has not be as extensively studied or validated, but nevertheless suggested to be an important predictor of behavior. For example, dual-task interference has been used as theoretical basis in a group-support system (GSS) context to explain why concurrently processing information from others while also contributing one’s own information to a discussion does not result in better decision making (Heninger et al. 2006). In

---

1 See Pashler (1994) for a brief literature review and summary of relevant theories relating to dual-task interference.
addition, dual-task interference has been used as a theoretical basis to explain how a lack of
cognitive fit in software maintenance may cause software developers to exhibit lower performance
on modification tasks (Shaft and Vessey 2006). In an end-user security setting, research has
suggested that just-in-time reminders may help alleviate the effects of dual-task interference, and
thereby improve users’ security behaviors (Jenkins and Durcikova 2013). Although models relating
to dual-task interference have been presented as a theoretical basis for past studies, research has yet
to understand and validate the degree to which dual-task interference actually influences different
types of security behaviors. This articles helps address this need through both theoretical
development and empirical validation.

**HYPOTHESIS DEVELOPMENT**

To explain how dual-task interference may influence secure behavior, this section
summarizes three theoretical perspectives of dual-task interference: the capacity sharing model, the
bottleneck (task switching) model, and the cross talk model (Pashler 1994). Based on these models,
we then explain how dual-task interference may decrease secure behavior when users’ both a)
perform security activities at the same time as other activities, and b) when other activities are
interrupted to perform security activities.

Three models are recognized as potential reasons why dual-task interference may decrease
performance in tasks: the capacity sharing model, the bottleneck (task switching model), and the
cross talk model. The capacity sharing model explains that dual-task interference is based on the
assumption that people share processing capacity (i.e., mental resources) among tasks (Tombu and
Jolicœur 2003). Because humans have finite cognitive resources (Marois and Ivanoff 2005; Sweller
1988), performance is impair when more than one task is performed together, as less cognitive
capacity is available for each individual task, (Tombu and Jolicœur 2003). People generally have
fair control of how they distribute their finite cognitive resources; when performing multiple tasks
simultaneously, they can choose which tasks to devote their limited cognitive capacity to (Pashler 1994). For example, in a phishing context, users can distribute their cognition to quickly and efficiently processing and responding to emails, or looking for cues of whether each email is legitimate or not. While it is common for users to give attention to both tasks, they will most likely devote more cognition to the primary task (checking and responding to emails), and less to secondary tasks (e.g., checking for phishing messages) (Pashler 1994).

Second, the bottleneck (task-switching) model explains that parallel processing may be impossible for certain mental operations (Dux et al. 2006; Pashler 1994; Sigman and Dehaene 2006). This model assumes that the mind has various mechanisms that are used to process information and perform operations. Some operations may simply require that the mind dedicate a mechanism to their processing for a short period of time. When one of the mechanisms is dedicated to performing an operation or processing information, it cannot be used to perform other operations or processes until it is available again. Thus, if two tasks require the same constrained mechanism at the same time, one or both of the tasks will be delayed or impaired (e.g., Navon and Miller 2002; Vandierendonck et al. 2010). This limitation is referred to as a bottleneck. For example, in a sensitive information disclosure scenario, if one is solving a complex analytical problem that involves sensitive information, one may not be able to simultaneously recall the regulations for protecting this information without switching attention away from the analytical problem. In this case, one would be more likely to disclose sensitive information without even noticing it. With any task, there could be a single or multiple bottlenecks that can affect performance.

Finally, the cross-talk model assumes that the content of information causes interference, not necessarily the mind’s limited processing capacities. Crosstalk is the communication between various sources of information, including sensory inputs, processes, and thoughts (Koch 2009; Navon and Miller 1987). This may include what a person is sensing from the environment, thinking about, or feeling from previous processing. The cross-talk model posits that concurrent tasks will
cause the mind to confuse the various sources of information. Information from one task will prime subsequent processing and behaviors in another task (Koch 2009). For example, if I am performing a work-related task that requires me to work quickly or efficiently, this mindset may influence my subsequent security activities—e.g., cause me to move more quickly through security even at the expense of weaker security. As another example, if I am using my computer for entertainment (e.g., movie watching or socializing) and visit a potentially non-secure website, my subsequent thoughts are more primed to recall feelings of enjoyment, rather than feelings of vulnerability. On the contrary, if I am doing tasks that are related to security and my mind is primed to be secure (e.g., watching a news report about a new virus), I am more likely to be primed to behave securely (positive cross-talk).

Building on these three theoretical perspective on dual-task interference, we explore how dual-task interference can influence two types of security activities: a) security activities initiated by the end-user that are performed simultaneously with other activities, called *simultaneous security activities*, b) security activities that are actively prompted from an outside source (e.g., the system) and interrupt users’ other activities to solicit a discrete response, called *discrete security activities*. We will now explain each of these activities separately.

*Simultaneous Security Activities*

Some security behaviors are simultaneously performed with other activities. Performing these types of security behaviors are most often initiated by the user, rather than prompted by a system. For example, while users check or respond to email, they must vigilantly screen for phishing emails (Burns et al. 2012). Or, when browsing websites and installing software, one must continuously assess the credibility of the website and software to avoid malware (Jin et al. 2009).

Per the three theoretical perspectives of dual-task interference, the performance of theses simultaneous-security activities are likely to be susceptible to dual-task interference as described below.
From a capacity sharing model, performing other activities at the same time as trying to perform simultaneous-security activities will decrease the amount of cognitive resources available to perform these security activities (as well as the other tasks). As a result, performance of these tasks generally drops (Tombu and Jolicœur 2003). For example, in a phishing context, if screening for phishing messages is performed at the same time as reading work-related emails, one may have less cognitive capacity to focus on identifying cues of phishing emails, and thereby be more likely to fall for phishing attempt. Likewise, from the perspective of the bottleneck model, if performing simultaneous-security activities requires the same cognitive resources as performing some other task, one will not be able to physically perform both tasks at once, and performance is likely to drop in the tasks (Dux et al. 2006; Pashler 1994; Sigman and Dehaene 2006). For example, if a user is cognitively absorbed in a task, and encounters a security threat, one may not even notice the security threat because the attention “bottleneck” is focused on the other task. Finally, from a cross-talk model, if a user is performing an activity that primes cognitions contrary to ideal security behaviors (e.g., primes a truth-bias that decreases perceived threat, primes a user to quickly complete the task at the expense of lower security, etc.), this may also have potential to decrease secure behavior (Koch 2009; Navon and Miller 1987). In summary, based on these three theoretical perspectives, we hypothesize:

H1. Performing security-related activities simultaneously with other activities will result in lower secure behavior than performing security-related activities alone.

Discrete Security Activities

The second type of activities that dual-task interference may influence are discrete-security activities. Discrete-security activities may include any intervention that discretely requests users’ attention to address a security need. These activities are not normally performed simultaneously with other activities, rather they are activities that require the users’ attention for a short period of
time to respond to the prompt. Examples of such activities includes responding to a virus warning or prompting the user to create a new password (Bravo-Lillo et al. 2011).

Although discrete-security activities are not always performed simultaneously with other activities, dual-task interference may still decrease their performance if they interrupt the other activities (e.g., Bravo-Lillo et al. 2011; Yee 2004). The premise for this possible relationship is that people may not be able to (or be willing to) free cognitive resources to ideally address the interrupting security prompt. For example, Yee (2004 p. 49) suggests, “interrupting users with prompts presents security decisions in a terrible context: it teaches users that security issues obstruct their main task and trains them to dismiss prompts quickly and carelessly”. Furthermore, Bravo-Lillo et al. (2011) suggest that interrupting prompts are often ignored or suboptimally addressed because users have a limited cognitive ability to switch between tasks and release needed resources. Hence, although a user’s attention is directed toward the security prompt, the user will often not free up cognitive resources to address the security need in anticipation of continuing the interrupted task afterwards. In other words, the mind keeps important elements of the primary task in short term memory, so that the activity can be easily resumed after addressing the security prompt.

This limitation of cognitive resource may decreases the amount of short-term memory available to evaluate and perform a prompted security action, resulting in dual-task interference. According to the capacity sharing model, this will decrease performance in the security behavior, even if the interference is small (Pashler 1994; Tombu and Jolicœur 2003). The consumption of resources may also present a bottleneck, or restrict access to needed resources to ideally perform the security behavior (Dux et al. 2006; Pashler 1994; Sigman and Dehaene 2006). Furthermore, if a security prompt interrupts an activity, this may result in frustration and thereby prime thoughts to avoid or hurry through the action (Bravo-Lillo et al. 2011; Yee 2004). This negatively primed thoughts may also have potential to decrease secure behavior, per the cross-talk model (Koch 2009).

In summary, we hypothesize:
H2. Interrupting other activities to perform security-related activities will result in lower secure behavior than performing security-related activities alone.

METHODOLOGY

In this section, we propose two experiments to test the hypotheses. The first experiment tests hypothesis 1 (simultaneous-security activities) and the second experiment tests hypothesis 2 (discrete-security activities).

PROPOSED EXPERIMENT 1

To explore how dual-task interference influences security behaviors that are performed simultaneously with other activities, a controlled experiment was designed in a phishing setting. A phishing context was chosen because checking for phishing messages is an activity that is frequently done while performing other tasks (e.g., reading and responding to legitimate emails). Furthermore, phishing has been identified as a serious threat to security that is rapidly growing (Symantec 2013). Subsequent experiments will focus on other types of secure behavior.

Experiment Task and Manipulations

The experimental task was designed to mimic a realistic scenario. Participants were told to role-play a new assistant for a manager, named Cameron Scott, at FrontSolutions, Inc. Prior to beginning their role, all participants were given a security-training video on how to avoiding phishing. The training video was approximately an 8 minute long narrated slide presentation (see Table 1 for example screenshots). It covered topics such as what is phishing, why it is important to identify phishing messages, phishing tactics (see Table 2 for example phishing tactics discussed), how to identify phishing messages, and examples of phishing messages. After the training, all participants were required to complete a short quiz that assessed their knowledge of phishing tactics.

2 Although this experiment has not been conducted yet, we wrote in past tense.
and how to identify phishing messages. All participants were required to get a perfect score on the quiz before continuing to verify they knew the material.

![Title page](image1)
![Example screenshot of phishing tactics](image2)
![Example screenshot of recognizing phishing tactics](image3)

**Table 1. Example screenshots from video**

<table>
<thead>
<tr>
<th>Phishing Tactics Discussed in Video</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Similar domain name</td>
<td>Annozon.com</td>
</tr>
<tr>
<td>Forms</td>
<td>A form asking for private information, such as a username or password</td>
</tr>
<tr>
<td>Disguised link</td>
<td><code>&lt;a href=&quot;185.34.52.111/login&quot;&gt;Wells Fargo&lt;/a&gt;</code></td>
</tr>
<tr>
<td>Request for sensitive information (e.g., passwords)</td>
<td>An email that requests the user to respond with sensitive information (e.g., a password, account number, etc.). This email may look like it is coming from a legitimate person.</td>
</tr>
<tr>
<td>Unknown attachments</td>
<td>An unanticipated attachment that contains malicious code.</td>
</tr>
</tbody>
</table>

After completing the training and passing the quiz, all participants were given the following scenario:
Role play that you are an assistant for Cameron Scott. Cameron Scott is a manager at Front Solutions, Inc. Among Cameron’s numerous duties, he is responsible for requesting/receiving financial information from the various departments at Front Solutions Inc., compiling financial reports, sending those reports to the CFO, and attending various meetings. All of his responsibilities are accomplished via email. He uses a company email address for receiving financial information, sending reports, and scheduling meetings. There are also times when he uses his company email for personal use. Currently, Cameron is expecting emails containing financial information (either attached to an email or embedded in an email) from 6 product division managers at Front Solutions.”

Participants were then randomly assigned to one of two conditions: a) a low dual-task interference condition or b) a high-dual task interference condition.

Low dual-task interference condition: In the low dual-task interference condition, participants were told that their sole task as Cameron’s assistant was to log into his email account to identify and delete any phishing emails. They were also warned not to delete any legitimate emails so that Cameron could review them later.

High dual-task interference condition: In the high dual-task interference condition, participants were told that they had two tasks. First, they were told to login to Cameron’s email account and fill out a financial summary sheet using information contained in the emails from the six product divisions (described in the general description). A template financial summary sheet was provide to the participants, which asked them to record the number of number of sales, total revenue, total costs, and then calculate the net revenue (revenue – costs). Second, they were asked to identify and delete any phishing emails in Cameron’s email account. They were also warned not to delete any legitimate emails so that Cameron could review them later.
Emails: After receiving their instructions, all participants were guided to a live online email account that was created specifically for this experiment. The inbox contained 20 emails. Six of the emails were from the product division managers (as mentioned in the general description given to both treatment groups); each of these emails contained sales and cost information for their product divisions. These emails contained none of the phishing characteristics discussed in the training (in the general description, participants were notified that Cameron was expecting these emails and they might contain legitimate attachments). Eight of the emails were random personal or company-related emails that contained none of the phishing characteristics discussed in the training. Six emails were phishing messages that contained at least one characteristic of a phishing message described in the training. Regardless of treatment, all participants received the exact same emails, in the same ordered. The emails are summarized in Table 3.

<table>
<thead>
<tr>
<th>Table 3. Emails contained in inbox</th>
</tr>
</thead>
<tbody>
<tr>
<td>Email 1: Other (email from family member)</td>
</tr>
<tr>
<td>Email 2: Division manager 1</td>
</tr>
<tr>
<td>Email 3: Phishing (unknown attachment)</td>
</tr>
<tr>
<td>Email 4: Other (email from bank)</td>
</tr>
<tr>
<td>Email 5: Division manager 2</td>
</tr>
<tr>
<td>Email 6: Other (email from work colleague)</td>
</tr>
<tr>
<td>Email 7: Division manager 3</td>
</tr>
<tr>
<td>Email 8: Phishing (request for password; forged senders address)</td>
</tr>
<tr>
<td>Email 9: Phishing (too good to be true)</td>
</tr>
<tr>
<td>Email 10: Other (email from work colleague)</td>
</tr>
</tbody>
</table>

Measuring Secure Behavior

After the experiment, two of the researchers logged into each account and recorded if the participant deleted each phishing email and also recorded if the participant deleted an email that was not phishing. This information was used to calculate an overall accuracy rate in detecting phishing messages as shown in Equation 1.
(number of true positive + number of true negatives) / (number of true positive + false positives + false negatives + true negatives)

OR

(number of true positive + number of true negatives) / total number of emails

number of true positives = Phishing emails that were deleted AND were the participant was not a victim (e.g., clicked on the phishing link, provided information, opened the phishing attachment)

number of true negatives = Legitimate emails that the user did not delete

Equation 1. Calculation of phishing detection accuracy

Participants and Data Analysis

At the time of this submission, data had not yet been collected. Before the workshop, the research team will have preliminary results to share. The analysis, performed using ANOVA, will explore whether the group with low dual-task interference will have higher phishing detection accuracy than the group with high dual-task interference.

PROPOSED EXPERIMENT 2

The second experiment was designed to test hypothesis 2—i.e., to test whether interrupting other activities to perform security-related activities will result in lower secure behavior than performing security-related activities alone. This experiment is thus relevant to discrete security activities (e.g., prompts that solicit users’ attention to complete a task such as creating a new password, updating virus protection, etc.). Secure behavior was operationalized as compliance with the password policy, and the interrupting prompt was operationalized as a request to create a new password. This operationalization was chosen as poor passwords represent one of the primary sources of large scaled security breaches (e.g., Hurtado 2011; Trustware 2012).

Experiment Task and Manipulations

The experiment was designed such that participants would interact with a realistic e-commerce website. Participants were asked to engage in a consulting task for a real e-commerce
organization that would require them to login to a live internet website and fill out an inventory report. The inventory report took about 15 minutes to fill out and involved completing a template with counts of products and simple calculations (e.g., starting inventory minus ending inventory). Participants were given a username and default password to access the system. However, they were told that at some point, they would be prompted to create a new password. The instructions then explained that creating a strong password was important to protect the organization, and therefore everyone is required to complete a training on the password security policy before accessing the system. Participants were presented a short training (a 5-minute narrated PowerPoint presentation) that explained how to create strong passwords. In addition, participants were required to pass a quiz on the content before beginning the task to ensure they comprehended the material. Afterwards, participants were randomly assigned to a high-dual task interference condition or a low dual-task interference condition. Content from the password policy is shown in Table 4.

<table>
<thead>
<tr>
<th>Table 4. Scoring Criteria for Compliance with Security Policy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criteria</td>
</tr>
<tr>
<td>Passwords should contain at least 15 characters</td>
</tr>
<tr>
<td>Passwords should contain both upper and lower case letters</td>
</tr>
<tr>
<td>Passwords should contain at least one special character</td>
</tr>
<tr>
<td>Password should contain at least one number</td>
</tr>
<tr>
<td>Password should not be a word found in a dictionary</td>
</tr>
</tbody>
</table>

**High dual-task interference condition:** After completing the training and quiz, participants in the high dual-task interference condition were allowed to log into the system and begin the task of filling in the inventory sheet. Exactly five minutes after starting the task (logging into the system), a popup window interrupted the activity and required participants to create a new password. After creating the new password, participants were allowed to complete the task.

**Low dual-task interference condition:** After completing the training and quiz, participants were asked to login to the system and watch an exactly five minute historical video about inventory management systems. The video did not contain any additional information about security that
would thereby influence participant’s subsequent password creation behavior. After the video was completed, participants were prompted to create a new password before they were allowed to start the task. The purpose of showing the video was to consume 5 minutes so that both treatment groups received the prompt to create a new password at the same time (e.g., the same duration of time sense watching the training video). However, because the video ended at 5 minutes, and participants had not yet started the inventory management task, the prompt to create a new password did not interrupt any activity. Rather, participants were able to focus on creating a strong password.

**Measuring Secure Behavior**

The dependent variable was compliance with the password security policy. When participants created their password, the system automatically calculated a score of how well the participant complied with the password policy, and stored this score in a database. The security policy contained five criteria for strong passwords; for each criteria, users received a score between 0 and 1 with a score of 5 indicating total compliance (see Table 5).

<table>
<thead>
<tr>
<th>#</th>
<th>Criteria</th>
<th>Score</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Passwords should contain at least 15 characters</td>
<td>( \frac{\text{# of characters in password}}{15} = 0...1 ) (capped at 1)</td>
</tr>
<tr>
<td>2</td>
<td>Passwords should contain both upper and lower case letters</td>
<td>1 if password contains upper and lower case number; 0 if it does not</td>
</tr>
<tr>
<td>3</td>
<td>Passwords should contain at least one special character</td>
<td>1 if password contains at least one special character; 0 if it does not</td>
</tr>
<tr>
<td>4</td>
<td>Password should contain at least one number</td>
<td>1 if password contains at least one number; 0 if it does not</td>
</tr>
<tr>
<td>5</td>
<td>Password should not be a word found in a dictionary</td>
<td>1 if password is not contained in dictionary; 0 if it is.</td>
</tr>
<tr>
<td></td>
<td>Total Possible Score</td>
<td>5</td>
</tr>
</tbody>
</table>

**Participants and Data Analysis**

At the time of this submission, data had not yet been collected. Before the workshop, the research team will have preliminary results to share. The analysis, performed using ANOVA, will
explore whether the group with low dual-task interference will have higher compliance with the password policy when prompted to create a new password than the group with high dual-task interference.

**DISCUSSION AND ANTICIPATED IMPLICATIONS**

This research explores how dual-task interference influences users’ secure behavior—i.e., compliance with organizational security policies and best practices. Based on the capacity sharing, bottleneck, and crosstalk theories of dual-task interference, we hypothesize that dual-task interference may decrease secure behavior in simultaneous-security activities (e.g., activities that a user performs on a continuous basis without being prompted, including assessing the credibility of websites, vigilantly looking for phishing attempts when checking email, etc.) and in discrete security activities that interrupt other activities (e.g., receiving prompts to create new passwords, to respond to a detected threat, or being actively prompted to perform other security activities in the middle of another task). To test these hypotheses, two experiments are proposed.

We expect to have preliminary results for the workshop. If the results of the experiment indicate that dual-task interference is a cause of sub-optimal security behaviors, this has both theoretical and practical implications. First, if the results hold, the research highlights a source of non-secure behavior that has not been sufficiently addressed in academic studies. In other words, this research establishes a foundation for future research to explore new theories and create interventions to alleviate the influence of dual-task interference in a security setting. For example, research has suggested that interventions such as reminders may help alleviate dual-task interference by directing users’ attention to security needs and providing them guidance on addressing these needs (Jenkins and Durcikova 2013). Pending on the results of this research, additional future research should explore other interventions that may alleviate the influence of dual-task interference on secure behavior.
Second, depending on the results of this research, theories of dual-task interference can be merged with other prominent theories of end-user security to potentially help account for more variance in secure behavior. Many of the theories thus far used to explain end-user security focus on a cognitivist approach to security—i.e., an approach that delineates people’s security behaviors are influenced by their beliefs and intentions. For example, protection motivation theory (PMT) (Rogers 1975) has been applied to a security context to predict that secure behavior is influenced by one’s intentions, which are influenced by beliefs regarding the severity, vulnerability, response-efficacy, and self-efficacy (e.g., Anderson and Agarwal 2010; Herath and Rao 2009; Johnston and Warkentin 2010; Siponen et al. 2006; Vance et al. 2012). Likewise, the theory of planned behavior (TPB) (Ajzen 1985) has been applied to a security setting to predict how secure behavior is again influenced by intentions, which are influenced by one’s attitude, subjective norms, and behavioral control (Bulgurcu et al. 2010; Dinev and Hu 2007; Ifinedo 2012). Theories on dual-task interference, however, focus less what one’s intentions and beliefs are, and rather on limitations of one’s physiological and cognitive capabilities (Pashler 1994), which may result in suboptimal security behavior. Therefore combining cognitivist theories of security (PMT, TPB, etc.) with theories of human limitations (e.g., dual-task interference) have potential to explain more variance in secure behavior.

Finally, from a practical perspective, this research has potential to inform practionaires regarding when users may be more vulnerable to security threats. Namely, if the hypotheses are supported, it will indicate that employees may be more vulnerable to disobeying security policies during busy, stressful, or other times when dual-task interference may be high. Security professionals and researchers can explore how to protect users during this time. For example, they can make sure that security prompts (e.g., changing passwords, backing up data, renewing security training) occur in less-busy times, or between tasks. Or, security professionals can even explore whether to deploy greater controls during times of high dual-task interference.
WORKS CITED


