Summer 6-15-2016

WHEN TRAINING GETS TRUMPED: HOW DUAL-TASK INTERFERENCE INHIBITS SECURITY TRAINING

Jeffrey L. Jenkins
Brigham Young University, jeffrey_jenkins@byu.edu

Bonnie Anderson
Brigham Young University, bonnie_anderson@byu.edu

Anthony Osborn Vance
Brigham Young University, anthony@vance.name

Scott Jensen
Brigham Young University, jensen.scott.r@gmail.com

WHEN TRAINING GETS TRUMPED: HOW DUAL-TASK INTERFERENCE INHIBITS SECURITY TRAINING

Research

Jenkins, Jeff, Brigham Young University, USA, jeffrey_jenkins@byu.edu

Anderson, Bonnie, Brigham Young University, USA, bonnie_anderson@byu.edu

Vance, Anthony, Brigham Young University, USA, anthony@vance.name

Jensen, Scott, Brigham Young University, USA, jensen.scott.r@gmail.com

Abstract

Security training programs are an important intervention to protect users and organizations against security threats. Unfortunately, users often ignore their training and engage in poor security behaviors. We explain how dual-task interference (DTI) is a primary cause of security training disregard. DTI is a cognitive limitation wherein humans cannot perform more than one task simultaneously without experiencing a deterioration of performance. In our context, we hypothesize how prompting users to perform security behaviors during high-DTI times may derail one's previous security training, resulting in less secure behaviors.

We test our hypotheses in an experiment that compares users' adherence to security training during low-DTI and high-DTI times in a realistic context. We found that performing security behaviors during low-DTI times increased adherence to prior security training by 31% compared to performing behaviors during high-DTI times. The results have implications for using DTI as a theoretical framework for understanding security behaviors, prompting users to perform security behaviors during times that will maximize adherence to past security training, and considering humans' neurological limitations when designing security training and intervention programs.

Keywords: Security training, dual-task interference (DTI), interruptions, user security behavior, security prompt timing.

1 Introduction

Security training programs are an important intervention to protect users against security threats (D'Arcy et al., 2009; Puhakainen and Siponen, 2010). For decades, numerous studies have shown that training can improve security behaviors, and studies have sought ways to improve the effectiveness of this training (e.g., Cox et al., 2001; Dodge et al., 2007; Furnell et al., 2002; Hollinger and Clark, 1983; Jenkins et al., 2012; Korpela, 2015; Schneier, 2005; Warkentin et al., 2011; Workman and Gathegi, 2007). However, despite users' positive intentions to follow their training, they often engage in noncompliant behaviors (Herold, 2009; Lincke, 2015; Schneier, 2005). This nonadherence to prior training can threaten the security of individuals and their organizations (Goel and Shawky, 2009). Thus, an important area of research is to better understand what factors may inhibit adequate security training from translating into positive security behaviors.

We propose that dual-task interference (DTI) may account for discrepancies between users' security training and their actual security behaviors. DTI is a neurological limitation wherein humans cannot perform more than one task simultaneously without experiencing a deterioration in performance (Pashler, 1994). This phenomenon is troublesome because users often are prompted to apply security-

training principles while in the middle of other primary tasks (e.g., using the computer for work, entertainment, or communication). Such interruptive behaviors are referred to as secondary tasks, and have been shown to cause DTI and thereby decrease performance in the primary task (Pashler, 1994). However, research has not yet examined how DTI also influences performance on the secondary task—i.e., the trained security behavior (see Figure 1). This is an important gap to address because the performance on the secondary task—the trained security behavior—is often considered more important than performance on the primary task. Thus, our first research objective is to understand how DTI influences people's performance on trained security behaviors.

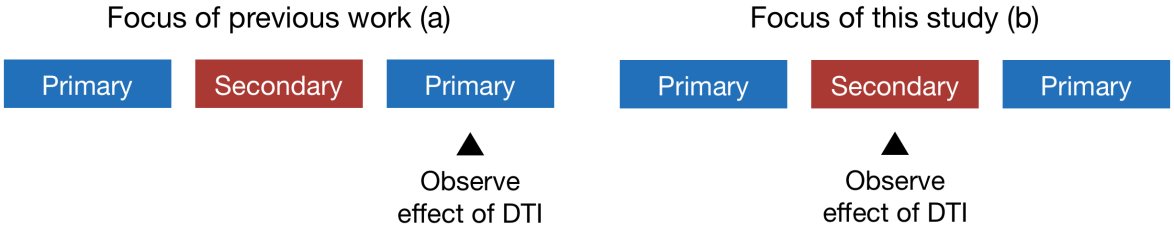

Figure 1. Observing the effect of DTI on the secondary security task (b) rather than the primary task (a).

We also propose that prompting users to perform security behaviors (e.g., choosing app permissions, updating software, resetting passwords, specifying privacy settings) during low DTI-times may help alleviate the discrepancy between security training and actual behavior. Although much research has been performed on improving the effectiveness of security training, little research has examined how the benefit of training can be maximized by prompting users to perform security behaviors when they are neurologically most capable of performing well (one of those timings being when DTI is low). In summary, the second objective of this research is to examine whether prompting users to perform security behaviors during low-DTI times (e.g., after a primary task) will result in higher adherence to security training than prompting users to perform security behavior during high-DTI times (e.g., during a primary task) (Figure 2).

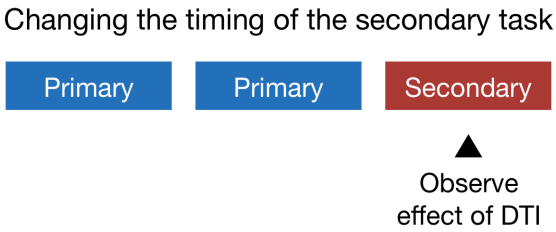

Figure 2. Observing the effect of DTI on the secondary task when it occurs after (rather than during) a primary task.

By addressing these research objectives, we make several contributions to research and practice. First, we theoretically and empirically demonstrate that DTI is an appropriate theoretical lens to understand security behaviors and that DTI may derail adequate security training causing users to behave non-securely. Second, we show that one way to mitigate the effect of DTI is to prompt users to perform security behaviors at low-DTI times. In our experiment, participants were 31% more compliant with their previous training when performing security behaviors during low-DTI times compared to high-DTI times. Finally, our research suggests that it is essential to account for human neurological limitations when designing effective security training and intervention programs.

2 Literature Review

DTI is a powerful theoretical lens for explaining why interruptions and concurrent tasks impact security behaviors. DTI theory explains performance decrements in a variety of contexts, including searching concurrently for multiple pieces of information (Navon and Miller, 1987), processing visual and verbal information together (Halbeisen and Walther, 2015), and switching attention between tasks (Szameitat et al., 2011). Normally, people are not aware of tasks interfering with each other unless the two tasks are cognitively difficult or physically incompatible. However, research shows that DTI can influence tasks that are "neither intellectually challenging nor physically incompatible" (Pashler, 1994). When people are involved in even simple cognitive tasks, they cannot process information or perform behaviors related to other tasks as quickly or as effectively (e.g., Duncan and Coltheart, 1987).

DTI is explained by two different paradigms: the bi-sensory and divided attention paradigm (Szameitat et al., 2011). Under the bi-sensory paradigm, people engage in two tasks simultaneously, such as walking and talking at the same time. In contrast, under the divided attention paradigm, participants must switch attention between stimuli (e.g., between an interrupting security message and a primary task). From a neurocognitive perspective, DTI in these paradigms is caused by tasks competing for the same brain functions (Rémy et al., 2010). When multiple tasks compete for the same cognitive functions, fewer resources are available for each individual task, and task performance subsequently decreases (Tombu and Jolicœur, 2003). Although a security message may interrupt and demand attention from a user for a short time, users do not necessarily free adequate cognitive resources associated with the primary task to respond effectively to the security message (Felt et al., 2012). DTI occurs as cognitive functions are still engaged in the primary task while performing the security task.

Although DTI has obvious implications for end-user security, it has not been extensively studied in security contexts. Several studies have alluded to the effects of DTI on security behaviors. Yee (2004) suggests that "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" (p. 49). One reason users choose to dismiss security advice quickly and carelessly in this context is because it is neurologically difficult for them to switch between their primary and security tasks. Further, research shows the vast majority of people do not pay attention to, notice, nor comprehend security advice in prompts (Akhawe and Felt, 2013). These findings suggest that cognitive functions associated with awareness and comprehension may be limited in the presence of dual-task interference. Further, security prompts and behaviors are often ignored or suboptimally addressed because users have a limited cognitive ability to switch between tasks (Bravo-Lillo et al., 2011).

DTI has been studied even less in a security-training context. As one notable exception, Jenkins and Durcikova (2013) introduce DTI as a possible deterrent of security behaviors, and suggest that DTI inhibits people from recalling training when making critical security decisions in an information disclosure context. They found that presenting training as just-in-time reminders helps overcome the effects of DTI because users are less reliant on the cognitive mechanisms of retrieving previously learned security information. However, this study did not actually manipulate DTI to explore how it influences security behaviors. Rather this study only used DTI as a theoretical lens to explain why just-in-time reminders are effective. Building on this research, we address two gaps. First, we empirically validate DTI as an appropriate theoretical lens to study security behaviors by directly manipulating DTI in a security context. Second, we examine how intelligent timing of security prompts can improve the translation of security training to positive security behaviors.

3 Hypothesis

In this study we attempt to quantify the effects of DTI by examining the percentage difference in security training adherence between high-DTI and low-DTI times. We examine whether prompting users to perform security behaviors during low-DTI times is a significant intervention for improving compliance with security training. Users frequently encounter interruptive security tasks during primary tasks. For

example, the Chrome browser has a cleanup tool, a prompt for which is triggered when Chrome detects malware. However, the timing of the tool's message causes overwhelming disregard (Google, 2015). As other examples, users are often prompted to reset passwords, update software, and remove adware at random intervals, many of which interrupt another task.

Prompting security messages in the middle of such tasks will be influenced by high-DTI and therefore inhibit people from recalling and implementing previous security training. Based on DTI theory (Pashler, 1994), when people are in the middle of a task and are interrupted by a secondary task, they must share limited cognitive resources between the tasks. As fewer cognitive resources are available for each task, performance on the tasks decreases, which may include remembering and implementing advice from past training. In such cases, users are neurologically incapable of optimally performing a security task consistently with previous training. In summary, these forms of DTI will result in security behaviors that are less compliant with previous training (Dux et al., 2006; Pashler, 1994; Sigman and Dehaene, 2006).

However, when prompts to perform security behaviors are intelligently timed so that they fall after a primary task (and before the beginning of the next primary task), users' cognitive and neurological resources are not consumed by the other task, and DTI will be low. In essence, the security task has a higher likelihood of being the solo primary task, and other tasks are not competing for attention. As a result, DTI is low and users have adequate resources to recall and implement past security training. In summary, we hypothesize:

H1. Users who are prompted to perform a security behavior after the completion of a primary task will be more compliant with their previous training than users who are prompted to perform a security behavior during the completion of a primary task.

4 Methodology

We designed a realistic study that examined how DTI influenced users' adherence to prior security training. We chose a password-creation scenario as a context to test the hypotheses. A password creation context was chosen because it is one of the most common ways that end-users interact with organizations to secure systems and resources, and it is also currently one of the greatest sources of large-scale security breaches, despite advances in security (e.g., Hurtado, 2011; Trustware, 2012). Importantly, it also allows us to measure objective compliance with the previous security training.

To test our hypothesis within this context, we designed a between-subject experiment with two treatments: (1) prompting users to create a new password in the middle of a primary task (the High-DTI condition) or (2) prompting users to create a new password after the completion of one primary task and before the beginning of another one (the Low-DTI condition).

4.1 Procedure

University students were invited to participate in a consulting agreement with a company as a part of a lesson on accounting information systems. The company was created by the research team for the experiment, but operated as a real company. For example, the company had its own domain, sold actual products online to real customers, and had business IT applications (e.g., email, an accounting information system, active directory, shared calendars, and online shared folders).

At the commencement of the consulting agreement, participants were told that because the business had access to sensitive financial data (which it actually did), they were required to complete a security training course prior to interacting with the company's systems. The training spanned two 90-minute class periods in a week (for a total of 180 minutes of training). During this training, participants were instructed regarding the mandatory password policy and other security information.

The policy explained that all passwords at the consulting-engagement company must meet a set of standards (listed below). After the training, participants were required to complete a quiz assessing their understanding of the password policy (reiterating each requirement in the policy). If participants did not

pass the quiz with 100% accuracy, they were required to study the password policy again and repeat the quiz until they passed it. The requirements stated that passwords should:

- contain at least 15 characters,
- contain both upper and lowercase letters,
- contain at least one special character,
- contain at least one number, and
- not be a word found in a dictionary.

After passing the training quiz, participants were given the password policy for reference and allowed to begin the consulting arrangement. The research team randomly assigned participants to one of the two treatment groups. The procedures for both groups are described below.

4.2 High-DTI Treatment

In the High-DTI treatment, participants were given instructions on how to complete their consulting engagement immediately after finishing the password security training. The consulting engagement required participants to compile a financial report based on information from various online company resources. Participants received a worksheet that gave them instructions on where to obtain the information. The cognitive flow of the task included retrieving instructions from the worksheet and, with these instructions in the users' working memory, access the specified online resource, pull information from that resource, and enter it into the worksheet. The company's online resources included a website, a shared folder, an online accounting information system, and email.

Approximately 5 minutes into the task, the instructions directed participants to access the online accounting information system to retrieve information regarding online sales. Upon logging into the system, participants were interrupted and prompted to create a new password. After creating a new password, they were allowed to access the information required to finish the task. As this interruption occurred during the task (as participants had instructions in their working memory to access the site) rather than between tasks (e.g., before starting the financial statement task), participants were required to create a password in the presence of High-DTI.

4.3 Low-DTI Treatment

In the Low-DTI group, participants watched an approximately 5-minute video on the history of e-commerce immediately after completing the required training but before starting their financial statement task. The video discussed how the Internet has revolutionized traditional commerce, but did not talk about security in any way. After the video, participants were told that they would shortly start their financial statement task but that before they could receive the worksheet with instructions, they needed to create a password to access the accounting information system. The purpose of watching the video was to help ensure that participants, regardless of treatment, would be prompted to create a password after approximately the same duration from receiving the security training (i.e., approximately 5 minutes). This helped to minimize the threat of a recency bias—i.e., one group performing better because they created the password sooner after receiving the training. As participants created the password between distinct primary tasks (after watching the video, but before starting the financial statement task), the level of DTI in this treatment would likely be lower than in the High-DTI treatment group. After creating the password, participants in the Low-DTI treatment group completed the same financial statement task as those in the High-DTI treatment.

4.4 Dependent Variable

The dependent variable was compliance with the password policy covered in the security training, which was automatically calculated as participants submitted their passwords. To calculate a compliance score, participants earned one point for each criterion with which they complied. For example, if the password was 15 characters or longer (the required length), the participant earned one point. If it was less than 15 characters in length, participants earned the value of the quotient (the number of characters divided by 15). Second, participants earned one point each for fulfilling the complexity requirements: having a password that contained both upper and lower case characters, at least one special character, and at least one number (for a total of three possible points). Finally, all passwords underwent a dictionary attack. If their password withstood the dictionary attack, participants earned one point. Thus, scores could potentially range from 0 (completely non-compliant) to 5 (completely compliant).

4.5 Participants

Two-hundred thirty-seven participants were recruited for the experiment from several introductory information systems courses and received class credit as part of a lesson on security and accounting information systems for participating. Participants were randomly assigned to a treatment group, resulting in 116 participants in the Low-DTI treatment and 121 participants in the High-DTI treatment. Approximately 68% of participants were male. The average age was 22.1, and participants had on average completed 2.4 years of higher-level education. Some 89% of participants were from the U.S. The three most represented disciplines were accounting (20%), business management (19%), and information systems (17%).

4.6 Analysis

We used an independent *t*-test to explore whether participants created more compliant passwords with their previous training in the Low-DTI treatment compared with the High-DTI treatment. The data was distributed normally, thus no transformation was performed. The means and standard deviations are shown in Table 1. The results indicated that participants created more compliant passwords in the Low-DTI treatment than in the High-DTI treatment (mean difference = .933; $p < .001$; $t(235) = 12.720$). Thus, our hypothesis was supported.

	N	**Mean**	**Standard Deviation**
High-DTI	121	3.009	.638
Low-DTI	116	3.942	.475

Table 1. Password compliance means and standard deviations

5 Discussion

This research sought to better understand how DTI influences people's performance on trained security behaviors. We found that performing security tasks during low DTI times significantly increased users' adherence to prior training in a password creation context by 31%. This finding demonstrates that prompting users to perform security behaviors immediately after a primary task and before beginning the next primary task is an effective timing to promote users to perform security behaviors consistent with their past training. This finding makes several contributions to research and practice.

First, we demonstrate that DTI influences security behaviors, and specifically the consistency of behavior with past training. Although past studies have suggested DTI as an appropriate theory to better understand security behavior (Jenkins and Durcikova, 2013), we directly test the influence of DTI on security behaviors through a simple manipulation (prompting users to perform a task in the middle of a

primary task compared to at the end of a primary task). We found that this simple manipulation significantly decreased users' compliance with their previous security training. Thus, we encourage future research to consider the application of DTI theory as an appropriate theoretical lens for studying security behaviors.

Second, we stress the need to prompt security behavior during low-DTI as opposed to high-DTI times to maximize the effectiveness of past training. Interestingly, many applications in practice are trending the opposite direction. For example, Android (as of version 6 Marshmallow) and iOS privacy prompts are displayed when the user data is first requested, rather than when an app is first installed (Tofel, 2015) and the Chrome clean up tool pops up semi-randomly. This is potentially problematic, because users are more likely to be engaged in a primary task when they are already using the software (which prompts the privacy notification) rather than before installing the app. Hence, Patil et al. (2015) found that interruptive privacy notices on mobile devices are poorly attended to. Our findings warn against this practice, and suggest that waiting after or before a primary task is a more appropriate time. This similar trend is observed with other security prompts including creating passwords, updating software, and removing malware. As a positive example of how our results can be applied, Microsoft's Skype gives users the option to update software when they are done using the program (e.g., when it closes)—an "after-the-task" time.

Third, our research stresses the importance in considering the neurology of the human when designing effective security training programs and interventions. Namely, although much valuable research has been conducted to design more effective training programs (e.g., Cox et al., 2001; Dodge et al., 2007; Furnell et al., 2002; Hollinger and Clark, 1983; Jenkins et al., 2012; Korpela, 2015; Schneier, 2005; Warkentin et al., 2011; Workman and Gathegi, 2007), these improvements may have limited effects on users' actual behaviors if the security decisions are presented at times that conflict with one's cognitive and neurological processing abilities (e.g., in times that have high DTI). Thus, our research reiterates the saying that "users are not the enemies" (Adams and Sasse, 1999), but rather have neurological limitations that must be considered when designing training and intervention security programs.

6 Limitations

This research has several limitations and boundary conditions that should be addressed in future research. First, our experiment only considered one type of security behavior—password creation. Future research should extend our findings to other types of behaviors (e.g., privacy prompts, security updates). A common practice is for password prompts to remind participants how to create strong passwords, partially reducing their reliance on past training. Past training however still provides valuable information on strategies and tactics for creating strong passwords in this scenario (e.g., how to create a passphrase). Importantly, even with reminder information, high DTI may still reduce password compliance as users are less able to deploy cognitive resources to generate a strong password. Future research should confirm this observation. Importantly, the finding that DTI decreases adherence to prior training is theoretically supported and should apply to various contexts.

As a second limitation, this experiment used student participants. This sample was designed to create homogeneity among participants that would reduce noise and thereby provide the strictest tests of the hypothesis (Calder et al., 1982). In addition, young people spend a comparatively large amount of time on personal computers and frequently experience security threats; therefore, they represent a valid sample. Finally, students engaged in a realistic task: they engaged in a real consulting project as a part of the class.

7 Conclusion

Security training plays an important role in mitigating security threats. However, too often, adequate security training does not translate to secure behaviors. We propose that dual-task interference is a theoretical lens that helps explain this gap. We found that performing security tasks during high-DTI times

substantially decreased adherence to prior security training. However, we found that prompting users to perform security tasks after a given primary task but before the next task is an effective way to mitigate DTI and maximize the effectiveness of the prior security training. Our results contribute to theory by validating DTI theory as an appropriate mechanism for understanding security behaviors. Further, from a practical perspective, we suggest that intelligent timing of security prompts help users better comply with their previous training. Importantly, our research also suggests the importance of accounting for human cognitive and neurological limitations when designing security training and interventions.

References

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

Akhawe, D., and Felt, A. P. 2013. "Alice in warningland: A large-scale field study of browser security warning effectiveness," in *Proceedings of the 22nd USENIX Conference on Security*, USENIX Association: Washington, D.C., pp. 257-272.

Bravo-Lillo, C., Cranor, L. F., Downs, J., Komanduri, S., and Sleeper, M. 2011. "Improving computer security dialogs," in *Proceedings of the 13th IFIP TC 13 International Conference on Human-Computer Interaction-Volume 6949 Part IV,* P. Campos, N. Graham, J. Jorge, N. Nunes, P. Palanque and M. Winckler (eds.), Springer-Verlag: Lisbon, Portugal, pp. 18-35.

Calder, B. J., Phillips, L. W., and Tybout, A. M. 1982. "The concept of external validity," *Journal of Consumer Research* (9:3), pp. 240-244.

Cox, A., Connolly, S., and Currall, J. 2001. "Raising information security awareness in the academic setting," *VINE* (31:2), pp. 11-16.

D'Arcy, J., Hovav, A., and Galletta, D. 2009. "User awareness of security countermeasures and its impact on information systems misuse: A deterrence approach," *Information Systems Research* (20:1) Mar, pp. 79-98.

Dodge, R. C., Carver, C., and Ferguson, A. J. 2007. "Phishing for user security awareness," *Computers & Security* (26:1), pp. 73-80.

Duncan, J., and Coltheart, M. 1987. *Attention and reading: Wholes and parts in shape recognition: A tutorial review*, England: Lawrence Erlbaum Associates, Inc: Hillsdale, NJ.

Dux, P. E., Ivanoff, J., Asplund, C. L., and Marois, R. 2006. "Isolation of a central bottleneck of information processing with time-resolved fMRI," *Neuron* (52:6), pp. 1109-1120.

Felt, A. P., Ha, E., Egelman, S., Haney, A., Chin, E., and Wagner, D. Year. "Android permissions: User attention, comprehension, and behavior," Proceedings of the Eighth Symposium on Usable Privacy and Security, ACM2012, pp. 3:1-3:14.

Furnell, S., Gennatou, M., and Dowland, P. 2002. "A prototype tool for information security awareness and training," *Logistics Information Management* (15:5/6), pp. 352-357.

Goel, S., and Shawky, H. 2009. "Estimating the market impact of security breach announcements on firm values," *Information & Management* (46:7), pp. 404-410.

Google (2015) Year One: Progress in the Fight against Unwanted Software. Google. Accessed 12/22/2015, https://googleonlinesecurity.blogspot.com/2015/12/year-one-progress-in-fight-against.html.

Halbeisen, G., and Walther, E. 2015. "Dual-task interference in evaluative conditioning: Similarity matters!," in *The Quarterly Journal of Experimental Psychology*, pp. 1-33.

Herold, R. 2009. "Common infosec & privacy training mistakes" January 30, 2013.

Hollinger, R. C., and Clark, J. P. 1983. "Deterrence in the workplace: Perceived certainty, perceived severity, and employee theft," *Social Forces* (62:2), pp. 398-418.

Hurtado, P. 2011. "Citigroup sued by cardholders over may security breach," Bloomberg.com *accessed 27 November 2015*

Jenkins, J. L., and Durcikova, A. 2013. "What, I shouldn't have done that? The influence of training and just-in-time reminders on secure behavior," in *International Conference for Information Systems (ICIS)*, AIS: Milan, Italy.

Jenkins, J. L., Durcikova, A., and Burns, M. B. 2012. "Forget the fluff: Examining how media richness influences the impact of information security training on secure behavior," *45th Hawaii International Conference on System Science (HICSS)*, IEEE, Maui Hawaii, pp. 3288-3296.

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

Lincke, S. 2015. *Organizing personnel security*, Springer.

Navon, D., and Miller, J. 1987. "Role of outcome conflict in dual-task interference," *Journal of Experimental Psychology: Human Perception and Performance* (13:3), p 435.

Pashler, H. 1994. "Dual-task interference in simple tasks: Data and theory," *Psychological Bulletin* (116:2), pp. 220-244.

Patil, S., Hoyle, R., Schlegel, R., Kapadia, A., and Lee, A. J. 2015. "Interrupt now or inform later?: Comparing immediate and delayed privacy feedback," in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, ACM: Seoul, South Korea.

Puhakainen, P., and Siponen, M. 2010. "Improving employees' compliance through information systems security training: An action research study," *MIS Quarterly* (34:4) Dec, pp. 757-778.

Rémy, F., Wenderoth, N., Lipkens, K., and Swinnen, S. P. 2010. "Dual-task interference during initial learning of a new motor task results from competition for the same brain areas," *Neuropsychologia* (48:9), pp. 2517-2527.

Schneier, B. 2005. "Insider threat statistics." www.schneier.com/blog/archives/2005/12/insider_threat.html *accessed 27 November 2015*.

Sigman, M., and Dehaene, S. 2006. "Dynamics of the central bottleneck: Dual-task and task uncertainty," *PLoS Biology* (4:7), p e220.

Szameitat, A. J., Schubert, T., and Muller, H. J. 2011. "How to test for dual-task-specific effects in brain imaging studies: An evaluation of potential analysis methods," *Neuroimage* (54:3) Feb 1, pp. 1765-1773.

Tombu, M., and Jolicœur, P. 2003. "A central capacity sharing model of dual-task performance," *Journal of Experimental Psychology: Human Perception and Performance* (29:1), pp. 3-18.

Trustware 2012. "Trustwave 2012 global security report " www.trustwave.com/Resources/Library/Documents/2012-Trustwave-Global-Security-Report/ *accessed 27 November 2015*.

Warkentin, M., Johnston, A. C., and Shropshire, J. 2011. "The influence of the informal social learning environment on information privacy policy compliance efficacy and intention," *European Journal of Information Systems* (20:3), pp. 267-284.

Workman, M., and Gathegi, J. 2007. "Punishment and ethics deterrents: A study of insider security contravention," *Journal of the American Society for Information Science and Technology* (58:2), pp. 212-222.

Yee, K.-P. 2004. "Aligning security and usability," *Security & Privacy, IEEE* (2:5), pp. 48-55.