Training Wheels: A New Approach to Teaching Mobile Device Security

Philip Menard
University of South Alabama, pmenard@southalabama.edu

Jordan Shropshire
University of South Alabama

Abstract
Despite massive investments in cyber security education, training, and awareness programs, most people retain unsafe mobile computing habits. They not only jeopardize their own data, but also risk the security of their associated organizations. It appears that conventional training programs are not ingraining sound security practices on trainees. This research questions the efficacy of legacy SETA frameworks and proposes a new cyber training tool for mobile devices. The tool is called Training Wheels. Training Wheels stands a number of cyber security training practices on their heads: instead of using punitive methods of reinforcement it provides rewards to encourage good behavior, instead of summary measures of security compliance it gives real-time feedback, and instead of isolating participants it displays participants' performance relative to their peers. These changes are grounded in established psychological theory. They are incorporated as key features of Training Wheels. Besides introducing the new training tool, this study also provides recommendations for its usage and implications for research.

Disciplines
Information Security | Management Information Systems | Technology and Innovation

INTRODUCTION

Employees and companies both have important motives for ensuring the security and integrity of mobile devices. People use mobile platforms to perform all manner of communications, retain troves of personal information, and conduct their private transactions. Smartphones have also become the primary business device for employees who travel often (Harris, Patten, & Regan, 2013). Therefore, organizational and individual data have become increasingly intertwined, with mobile device security becoming more important for organizations. Enterprise data, connectivity tools, and access to organizational resources are often available via handheld device. Loss of control over devices and data has the potential to be financially devastating for both the individual and the organization (Kwon & Johnson, 2014). Identity theft may result in criminals gaining access to bank and retirement accounts or applying for credit with victims' credentials. Mobile devices are also an access point to corporate resources such as email, instant messaging, databases, file shares, and other hosted apps. However, security breaches are not only financially detrimental; an organization's reputation may also be damaged. Organizations which fall victim to security breaches often observe an immediate and enduring loss of consumer trust, curtailing sales for extended periods of time (Gross, 2013). Training mobile device users to minimize their threat profile remains the best method for preventing such losses (Harris et al., 2013).

Security Education Training and Awareness (SETA) programs are an important preventive measure against security breaches (Straub & Welke, 1998). They increase users' awareness of risks and describe safe ways to use computing devices. SETA programs are normally based on policies created by organizations to urge secure device usage among their employees. Awareness programs usually focus on a series of seminars conducted for groups of employees (Guttman & Roback, 1995; Hansche, 2001a, 2001b). During the seminars, the employees are usually apprised of the risks to themselves and the organization. Based on the policy in place, they may also be warned of punishments or sanctions for failing to fully comply with security protocols. The sanctions may fluctuate but are based on criminological models for deterring unwanted behavior (D'Arcy & Herath, 2011; D'Arcy, Hovav, & Galletta, 2009; Herath & Rao, 2009; Siponen & Vance, 2010). Awareness sessions are sometimes followed by quizzes to assess participants' retention of the security concepts. This typical implementation of SETA has been adapted with little change for nearly three decades (Guttman & Roback, 1995; Murray, 1991) and has not demonstrated much success. Researchers have continually shown that this method has little influence on the actual behavior of SETA participants (Eyadat, 2015).

One of the more pressing issues with most SETA programs are that they are created with economies of scale in mind (Eyadat, 2015). For example, most SETA programs are designed to be delivered to as wide an audience as possible and to be used for as long as possible. Many large organizations have just one SETA program that every employee must fulfill (Eyadat, 2015). This builds efficiency by reducing costs, simplifying design, and easing course distribution. It also results in the type of static, generic content that people tend to ignore.

In this study, we propose a new direction in SETA. These changes are manifested in a mobile device-based tool called Training Wheels. Rather than emphasizing cost containment, Training Wheels is focused on maximizing relevance to trainees. Using this approach, levels of immediacy and specificity not seen in other frameworks can be attained. Micro training sessions are delivered as individuals use their devices. Compliance is assessed at the level of the individual behavior. Feedback is presented as a single composite score which is updated in real time and provided within the context of one's peers. Rewards for compliance are given instead of punishments for noncompliance, and they are awarded based on specific behaviors. We expect that these differences will lead to real changes in peoples' behavior within the mobile ecosystem.

We propose Training Wheels as an extension of the Android operating system that has visibility and control over the entire ecosystem. In this study, we describe the design and intended applications of Training Wheels. Because the features developed for Training Wheels are based on psychological theory, we also provide a theoretical background on motivational psychology, emphasizing how important motivational factors are implemented as key features. The remainder of this manuscript is organized as follows: the following section provides the background. It describes trends and commonalities among contemporary SETA programs. The following section underscores Training Wheels' psychological underpinnings. Specifically, it reviews the intrinsic and extrinsic motivational factors which impact the design. The next section introduces the new approach. After giving a brief overview, it discusses the design goals and then outlines the organization of the software. The next section describes the recommended applications for the proposed approach. Finally, implications for research and final conclusions are shared.

BACKGROUND

SETA programs have traditionally been operationalized as mandatory, periodical (usually annually) seminars intended to increase awareness of information security policy components among employees. These awareness programs typically disseminate information though some combination of lectures, videos, or handouts (Murray, 1991), with retention measured using post-SETA

quizzes. Advanced versions of SETA programs are training programs (demonstration and hands-on practice) and education programs (outside reading, discussion, and independent research) (Guttman and Roback, 1995). Most organizations do not require their employees to attain knowledge beyond general policy awareness programs despite the long-term impact of training or education programs (Menard, 2015). Examples of common SETA implementations are detailed in Table 1. Although this table does not represent the breadth of SETA research, it does demonstrate the lack of evolution in current SETA programs compared with previous iterations, with most taking a one-size-fits-all approach. As a result, employees often do not recognize the relevance of their SETA program, either because the program is boring or out of context (Caldwell, 2016).

Program	Description	Purpose	Source
Traditional SETA	Combination of courses, seminars, videos, handouts, directives, reminders, newsletters	Provide baseline information for understanding security issues	Murray, 1991
Repeated SETA participation	Recommends role-playing, reviewing case studies, or showing a security videos	Ongoing SETA for influencing employee behavior	Mitnick & Simon, 2002
Online training	Web-based training. A series of textual modules are presented to all trainees. A quiz is offered after every module.	To maintain compliance with Federal security training requirements for contractors.	Jones and Pardehava, 2007
"Hypermedia"	Combination of text-based learning and multimedia for educating employees on security practices	Improve employees' learning of security by providing information in a richer format	Shaw et al., 2009
Motivational SETA	Traditional text- and video-based SETA program with motivational manipulations embedded	To determine if employees can be intrinsically motivated to participate in an awareness program	Menard, 2015

Table 1: Sampling of Research to Demonstrate Typical SETA Programs

TRAINING WHEELS: A NEW APPROACH

This research proposes a behavioral modification tool which is operationalized as an extension of the Android operating system. The proposed tool is called Training Wheels because it initially locks down most Android features and provides graduated levels of more autonomy as safe behavior is observed. The first time the user attempts to use an ecosystem feature (such as onboard camera or downloading an app) he or she is prompted to complete a micro-training session. These animated training sessions are designed to open in a new window and last for no longer than 20 seconds. They highlight security risks and describe safe use of the feature. After training, limited use of the feature is then granted. In addition, Training Wheels provides reminders each time the feature is used. The feature is unlocked only after a number of instances of safe usage are observed. Thus, the incentive to adopt security recommendations is the reward of increased autonomy. Training Wheels assesses each instance of a feature-usage. A composite compliance score is updated is real-time. To provide context, a leaderboard which tracks the scores of peer users is also available.

In this section, the psychological underpinnings are first delivered. These are the requirements of successful SETA programs. The psychological aspects became design goals around which Training Wheels was developed. The second section describes the actual design goals. The third section introduces the technical implementation.

Psychological Underpinnings

Each of the features incorporated in Training Wheels addresses an important psychological factor which is often discussed by researchers but rarely operationalized for training. The following sections describe the motivational theory that informs the inclusion of our training features.

Intrinsic Motivation

Intrinsic motivation has been shown to be critical to student achievement and success in educational scenarios (Vallerand, 1997). As a result, it may also be important in forming individuals' desires to learn about information security. Motivation is traditionally categorized as intrinsic or extrinsic (Deci, 1972; Ryan & Deci, 2000). Intrinsic motivation is the performance of an activity for the pleasure or satisfaction attained during engagement (Vallerand, 1997). Researchers have classified specific forms of intrinsic and extrinsic motivation (Ryan & Deci, 2000). Intrinsic motivation may manifest as intrinsic motivation to know, intrinsic motivation to achieve, and intrinsic motivation to experience stimulation (Vallerand, 1997). Intrinsic motivation to know is the engagement in an activity for

the gratification that one experiences while understanding a new concept. Intrinsic motivation to achieve is engagement in an activity with the intent of bettering oneself. Intrinsic motivation to experience stimulation is the engagement in an activity to experience pleasant or enjoyable sensations. When applied to the context of a SETA program, an employee's participation due to a desire to learn more about information security is an example of intrinsic motivation (Menard, 2015).

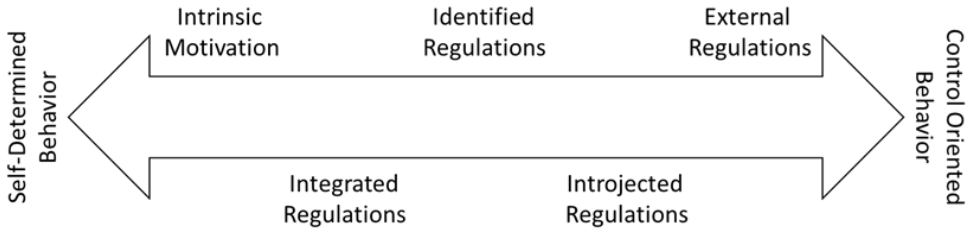

Figure 1: Types of Motivation along the Self-Determined Continuum

Extrinsic Motivation

Extrinsic motivation is participating in an activity as a means to an end and not for its own sake (Vallerand, 1997). Because prior research that classified intrinsic and extrinsic motivation as dichotomous yielded mixed results, Deci and Ryan (1980) developed Self-Determination Theory (SDT), which identifies specific types of extrinsic motivation that are placed on a self-determined spectrum (see Figure 1). Self-determination is the degree to which someone's motivation is internalized. External regulation refers to being motivated by rewards or sanctions. Introjected regulation refers to the shame or satisfaction someone perceives based on the admonishments or compliments given by important others. Identified regulation means that the behavior being performed, while not completely self-determined, is a means to performing some other behavior that is self-determined (i.e. an extrinsic means to an intrinsic end). Integrated regulation means that an individual views a behavior, even if it is not completely intrinsically derived, as an extension of the individual.

External regulation has been indirectly studied in security research through the adaptation of General Deterrence Theory and the inclusion of sanctions in information security policies (D'Arcy et al., 2009; Goodhue & Straub, 1991; Straub, 1990). With policy sanctions, an employee would be motivated to perform behaviors purely to avoid reprimands. Although the avoidance of punishment may influence an employee's intention to comply with a policy, motivational research has shown that there are substantial benefits when someone is intrinsically motivated, including more positive attitude and better cognition (Vallerand, 1997). SETA programs offer an obvious opportunity to intrinsically motivate employees.

SDT also models motivation as being influenced by an individual's perceptions of autonomy, competence, and relatedness (Deci & Ryan, 1980). Autonomy is the degree to which one has the freedom to choose an activity being performed. Competence is the degree to which one can produce desired outcomes or prevent undesired consequences. Relatedness is the degree to which one feels connected with other people or things, either emotionally or through social interaction (Vallerand et al., 1997). Autonomy, relatedness, and competence increase intrinsic motivation and decrease control-oriented forms of extrinsic motivation (Deci & Ryan, 1980; Ryan, Mims, & Koestner, 1983; Vallerand, 2000).

The design features embedded the proposed SETA program are crafted to emphasize each of the psychological factors that influence intrinsic motivation. They are: (1) a composite score, ranging from 0-100 and updated in real time, based on how secure a person's behaviors are in total; an explanation of the factors contributing to the score is also provided (2) Initial lockdown of features upon starting the training, with features being unlocked as training modules are completed and good behavior is captured (i.e. as your score goes up, more features are unlocked) (3) a leaderboard that shows how everyone using the software is ranked based on their composite score (4) a personalized appeal embedded within each training module to establish security relevance (i.e. a module on password strength would highlight various weaknesses in a password stored on the device and state how quickly a hacker can determine the password through brute force).

The composite score addresses "competence" – people become more intrinsically motivated to learn as timely positive feedback is provided in response to an action. The locking and unlocking of features addresses "autonomy" – as people are granted more freedom, they become more intrinsically motivated. The leaderboard and personalized appeals both address aspects of "relatedness," which has both social and emotional components. The leaderboard increases people's social interaction as they use the software and should elicit friendly competition. The personalized appeal creates an emotional connection between the person and his/her information by demonstrating how specific information on the device could be compromised. The personalized appeal also addresses prior issues with people recognizing the relevance of security threats. Machine learning will also be incorporated in the software by analyzing trends in device usage and delivering personalized, on-the-spot training to prevent an unsecure action.

Design Goals

The aforementioned psychological underpinnings are necessary elements of SETA programs. In order successful training organizational members, they must be met. Unfortunately, many contemporary programs for mobile device users fall short of meeting these expectations. Therefore, this research proposes several

advances in cyber training. Most SETA programs focus on mass delivery of training content because their goal is to contain costs and simplify administration. However, the primary design goal here is to maximize the relevance of the training with respect to the user. It maximizes content relevance by limiting training to only deliver content which is specific to the device feature be used by the trainee. It maximizes temporal relevance by providing real-time training, assessment, and feedback of user behavior. A secondary design goal is to offer positive reinforcement instead of just negative reinforcement. While the majority of cyber training programs emphasis punishment and sanctions for undesired behavior, the proposed program rewards desired behavior. The reward is relevant to a specific behavior, as it mostly takes the form of additional autonomy in the use of the related system feature. Further, each individual behavior has an impact on the trainee's composite compliance score. This real-time score is presented as a percentage, with higher percentages equating to higher levels of compliance. To add context and foster competition, a leaderboard is also updated in real-time. The board depicts the scores of the trainee's peers, so each trainee will know how well he or she is doing relative to other trainees.

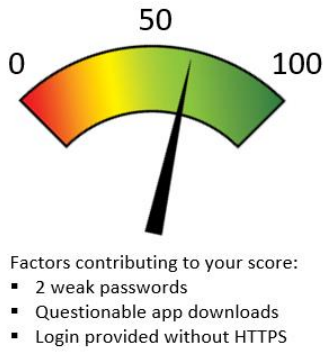

Figure 2: Example of composite score feature

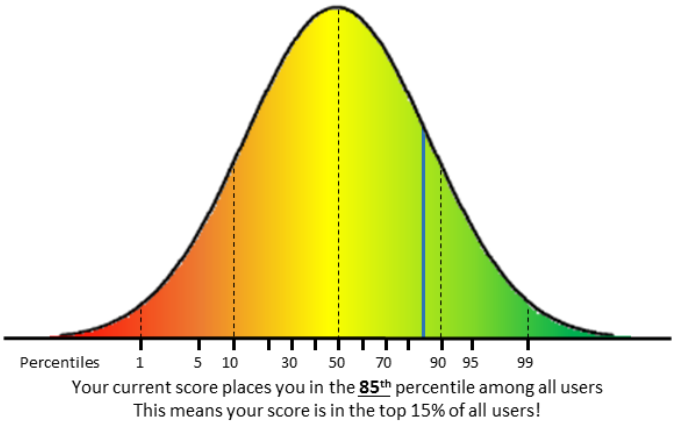

Figure 3: Example of leaderboard feature

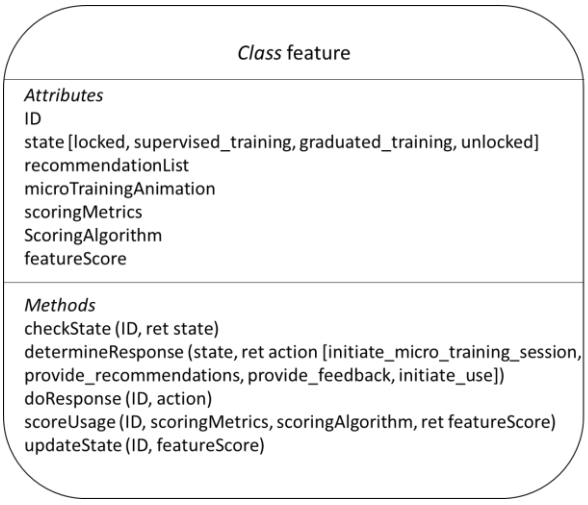

Figure 4: Class Feature Definition

Technical Description

Training Wheels is proposed as a modification of Android 6.0.1, the latest stable release of the operating system. The additional software will be written with a combination of C++ and JAVA. It intercepts syscalls from the system libraries and userspace applications and maps each call to a corresponding process. Each process is then linked to an instance of feature classes (see Figure 4). A feature class refers to a set of mobile device features for which there will be specific security cues. For example, change_password, check_email, send_SMS, download_app, and activate_Bluetooth are classes of features. The status of each feature is checked against a corresponding lookup in real time. A feature's status will be one of state [locked, supervised_training, graduated_training, unlocked] according to usage history. The result of each feature usage request will be one of action [initiate_micro_training_session, provide_recommendations, provide_feedback, initiate_use], based on feature status. In all but the last case, the proc is suspended until the response is complete. After a feature is used (e.g., password is changed) the user's behavior is scored. Each feature class has behavioral attributes which are empirically assessable. For instance, feature change_password may quantify password length, difficulty, and recency of each password. These values are summarized using a weighted scoring algorithm unique to the feature class. The resulting value is the score for the feature class. The feature status is upgraded when the feature score exceeds a threshold value for a predetermined number of feature uses. The composite score is an average of the scores of the feature classes. The initial stages are presented in Figure 5 (below).

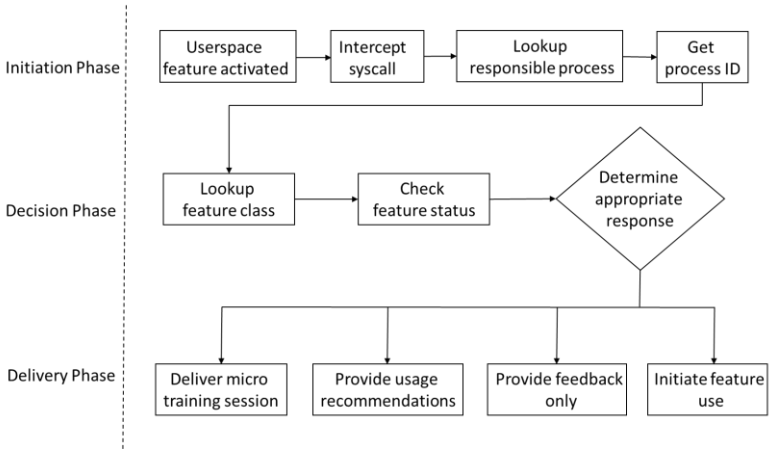

Figure 5: Response to Feature Request

RECOMMENDATIONS FOR USAGE

The final version of the Training Wheels software will be available as an open source fork of the Android OS, available on GitHub. It is recommended that enterprises which provide mobile devices to their employees preload the software onto every device. The training program can be modified to include security policies which are unique to the organization. This allows for a more complete implementation of security strategies. Because Training Wheels is a full version of the Android operating system, an organization could require its employees to install it on their mobile devices as a condition of their employment. The delivery and installation could be managed using a localized patch management server. Many organizations require their employees to install corporate applications which provide insight into employee activities. Given that a precedent already exists, this software does not break new ground or evoke unsettled legal issues.

IMPLICATIONS FOR RESEARCH

Information security research has extensively examined how deterrence influences employees' behavior. One problem with researchers' adaptation of deterrence theory for information security contexts is the mismatch of its origins in criminology (Crossler et al., 2013; D'Arcy & Herath, 2011) and the actual severity of a policy violation. Most noncompliance behaviors cannot be equated to criminal activity. A contribution of this research may be its offering of a counterpoint to deterrence research. By intrinsically motivating the performance of employees' secure behaviors, we may demonstrate the validity of adapting motivational theory in the information security research domain. This work may also present interesting

future research avenues related to alternative methods of motivating individuals to behave more securely.

One of the important propositions in motivational research is the recursive nature of motivational influence (Vallerand, 1997). For example, if an employee is continually intrinsically motivated while performing different tasks at work, the employee's motivation toward the entire workplace context will become intrinsic. Top-down effects (contextual to situational motivation) can be measured using cross-sectional data, but bottom-up recursive influence is formed as the employee experiences motivational perceptions while performing different tasks. This research is designed to capture behaviors and perceptions over time through a mobile SETA program and can inform both security and motivational research about the effects of the persistent incorporation of intrinsic motivation.

While organizational policy mandates have been examined in information security studies (Boss, Kirsch, Angermeier, Shingler, & Boss, 2009; Smith, Winchester, Bunker, & Jamieson, 2010), mandates have yet to be examined in the context of SDT and SETA programs. Placing a mandate on employees' participation in both an awareness and training program may yield interesting results. For example, a mandate may negatively affect an employee's self-determination and produce control-oriented perceptions among employees. A mandatory SETA program could also diffuse the influence of embedded motivational enhancements within the program.

Because training has more enduring impacts on employees than awareness, intrinsically motivating employees to learn about information security through both awareness and training programs may demonstrate long-term effects on the performance of secure behaviors. Because the present study is longitudinal in nature, our study is capable of capturing important behavioral information that would not be measured in research designs of most SETA studies.

LIMITATIONS AND FUTURE RESEARCH

One potential limitation is possible user resistance if implemented in an organization. Employees may not appreciate having their privileges initially revoked and then unlocked with compliant behavior. This issue could be mitigated with an introductory training session, where employees are issued their mobile devices with Training Wheels and are then walked through a demonstration of how the training works. By participating in this initial demonstration session and viewing several micro-training videos as examples, many of the features most important to employees' daily work will be unlocked. The composite score feature can also include a list of any features that are in danger of being locked due to a return to non-compliant behavior, giving employees a chance to better align their

behaviors with policy before privileges are revoked. Although not a perfect solution, this approach is similar to the implementation of standard organizational security policies which require employee participation in a SETA program before further use of computing devices. Training Wheels has the added benefit of equipping employees with additional knowledge about security as behavior is observed. With Training Wheels offering continuous training throughout the use of the device, the initial demonstration session will not need to be as time-consuming as a typical SETA program. Additionally, employees will have a better understanding of the reasons for policies and how to align their behaviors accordingly.

It should be noted that the proposed system was designed for organizations in industrial sectors in which high security is the norm. For instance, workers in the healthcare, banking, and defense industries are often expected to participate in training as a condition of their employment. Training Wheels may be most appropriate for these scenarios.

Another potential limitation is the exclusive use of Android as a development platform. However, the features described in this paper are not heavily reliant on Android-specific functionality. Our framework can be extensible to other operating systems, but as an open source platform, Android offers the best opportunity for initial development and testing. The psychological theory that serves as the foundation of Training Wheels should be applicable regardless of the platform.

CONCLUSION

In the past, organizations have opted for a one-size-fits-all, cost-containment strategy for delivering cyber training. A single, static course is usually delivered to everyone in the enterprise. The effectiveness of this approach is questionable. Research has shown that even after completing training, few individuals actually modify their own behavior. We suspect that the lack of relevance precludes real change. This manuscript describes a new approach to SETA. Unlike previous approaches, it maximizes relevance to the individual - relevance in terms of content and relevance in terms of delivery time. These changes are manifested in a new training tool called Training Wheels. Training Wheels offers real-time recommendations based on observations of user behavior. It also integrates a real-time feedback mechanism and offers incentives which correlate to specific behavioral changes. Although Training Wheels has been designed and prototyped, its relative efficacy has not yet been established. In the near future, a split-half style experiment will be conducted to ascertain its effectiveness at changing peoples' behavior. The results of the experiment are expected to confirm the validity of the relevance-based approach to security education and training.

REFERENCES

Boss, S. R., Kirsch, L. J., Angermeier, I., Shingler, R. A., & Boss, R. W. (2009). If Someone is Watching, I'll Do What I'm Asked: Mandatoriness, Control, and Information Security. *European Journal of Information Systems*, *18*, 151–164. article. http://doi.org/10.1057/ejis.2009.8

Caldwell, T. (2016). Making security awareness training work. *Computer Fraud & Security*, *2016*(6), 8–14. http://doi.org/10.1016/S1361-3723(15)30046-4

Crossler, R. E., Johnston, A. C., Lowry, P. B., Hu, Q., Warkentin, M., & Baskerville, R. (2013). Future Directions for Behavioral Information Security Research. *Computers & Security*, *32*(1), 90–101.

D'Arcy, J., & Herath, T. (2011). A Review and Analysis of Deterrence Theory in the IS Security Literature: Making Sense of the Disparate Findings. *European Journal of Information Systems*, *20*(6), 643–658. article. http://doi.org/10.1057/ejis.2011.23

D'Arcy, J., Hovav, A., & Galletta, D. (2009). User Awareness of Security Countermeasures and Its Impact on Information Systems Misuse: A Deterrence Approach. *Information Systems Research*, *20*(1), 79–98. article. http://doi.org/10.1287/isre.1070.0160

Deci, E. L. (1972). The Effects of Contingent and Noncontingent Rewards and Controls on Intrinsic Motivation. *Organizational Behavior and Human Performance*, *8*(2), 217–229. http://doi.org/10.1016/0030-5073(72)90047-5

Deci, E. L., & Ryan, R. M. (1980). The Empirical Exploration of Intrinsic Motivational Processes. In L. Berkowitz (Ed.), *Advances in Experimental Social Psychology* (pp. 39–80). New York: Academic Press.

Eyadat, M. (2015). The Impact of SETA Program on Organizational Information and Performance. In *Proceedings of the 27th Annual CSU-POM Conference* (pp. 45–54).

Goodhue, D. L., & Straub, D. W. (1991). Security Concerns of System Users: A Study of Perceptions of the Adequacy of Security. *Information & Management*, *20*(1), 13–27. article. Retrieved from http://www.sciencedirect.com/science/article/pii/037872069190024V

Gross, D. (2013). Report: Eastern European Gang Hacked Apple, Facebook, Twitter. Retrieved from http://www.cnn.com/2013/02/20/tech/web/hacked-apple-facebook-twitter/index.html

Guttman, B., & Roback, E. A. (1995). *An Introduction to Computer Security: The NIST Handbook*. U.S. Department of Commerce. Retrieved from http://csrc.nist.gov/publications/nistpubs/800-12/handbook.pdf

Hansche, S. (2001a). Designing a Security Awareness Program: Part I. *Information Systems Security*, *9*(6), 14–22.

Hansche, S. (2001b). Information System Security Training: Making It Happen: Part 2 of 2. *Information Systems Security*, *10*(1), 48–56.

Harris, M. A., Patten, K., & Regan, E. (2013). The need for BYOD mobile device security awareness and training. In *Proceedings of the Nineteenth Americas Conference on Information Systems*.

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. article.

Kwon, J., & Johnson, M. E. (2014). Proactive Versus Reactive Security Investments in the Healthcare Sector. *MIS Quarterly*, *38*(2), 451–471.

Menard, P. (2015). *The Influence of Self-Determined Motivation on Security Education Training and Awareness (SETA) Programs*. Mississippi State University.

Mitnick, K. D., & Simon, W. L. (2002). *The Art of Deception: Controlling the Human Element of Security*. New York: Wiley Publishing, Inc.

Murray, B. (1991). Running Corporate and National Security Awareness Programs. In *Proceedings of the IFIP TC11 Seventh International Conference on IS Security* (pp. 203–207). Amsterdam: North-Holland Publishing Co.

Ryan, R. M., & Deci, E. L. (2000). Intrinsic and Extrinsic Motivations: Classic Definitions and New Directions. *Contemporary Educational Psychology*, *25*(1), 54–67. http://doi.org/10.1006/ceps.1999.1020

Ryan, R. M., Mims, V., & Koestner, R. (1983). Relation of Reward Contingency and Interpersonal Context to Intrinsic Motivation: A Review and Test Using Cognitive Evaluation Theory. *Journal of Personality and Social Psychology*, *45*(4), 736–750.

Siponen, M., & Vance, A. (2010). Neutralization: New Insights into the Problem of Employee Information Systems Security Policy Violations. *MIS Quarterly*, *34*(3), 487–502. article.

Smith, S., Winchester, D., Bunker, D., & Jamieson, R. (2010). Circuits of Power: A Study of Mandated Compliance to an Information Systems Security De Jure Standard in a Government Organization. *MIS Quarterly*, *34*(3), 463–486. article.

Straub, D. W. (1990). Effective IS Security: An Empirical Study. *Information Systems Research*, *1*(3), 255–276. article.

Straub, D. W., & Welke, R. J. (1998). Coping With Systems Risk: Security Planning Models for Management Decision Making. *MIS Quarterly*, *22*(4), 441–469. article.

Vallerand, R. J. (1997). Toword A Hierarchical Model of Intrinsic and Extrinsic Motivation. *Advances in Experimental Social Psychology*, *29*, 271–360.

Vallerand, R. J. (2000). Deci and Ryan's Self-Determination Theory: A View From the Hierarchical Model of Intrinsic and Extrinsic Motivation. *Psychological Inquiry*, *11*(4), 312–318.

Vallerand, R. J., Fortier, M. S., & Guay, F. (1997). Self-Determination and Persistence in a Real-Life Setting: Toward a Motivational Model of High School Dropout. *Journal of Personality and Social Psychology*, *72*(5), 1161–1176. Retrieved from http://www.ncbi.nlm.nih.gov/pubmed/9150590