Traditional SETA No More: Investigating the Intersection Between Cybersecurity and Cognitive Neuroscience

Humayun Zafar, Ph.D.
Kennesaw State University
hzafar@kennesaw.edu

Adriane Randolph, Ph.D.
Kennesaw State University
arandol3@kennesaw.edu

Saurabh Gupta, Ph.D.
Kennesaw State University
sgupta7@kennesaw.edu

Carole Hollingsworth, Ph.D.
Kennesaw State University
chollin2@kennesaw.edu

Abstract

We investigated the role automated behavior plays in contributing to security breaches. Using different forms of phishing, combined with multiple neurophysiological tools, we were able to more fully understand the approaches participants took when they engaged with a phishing campaign. The four participants of this pilot study ranged in their individual characteristics of gender and IT experience while controlling for age. It seems the biggest factor for awareness and successfully resisting a phishing campaign may be proximity of security training to engagement with that campaign. Neurophysiological tools helped illustrate the thought processes behind participants' statements and actions; combined with consideration of individual characteristics, these tools help shed more light on human behavior. In the future, we plan to further enhance our testing environment by incorporating an emergent model that considers work task complexity and incorporate more industry participants with a range of IT experience.

1. Introduction

Samantha needed to work on a large file at home. It was too big to email, so she absent-mindedly plugged a flash drive someone had left in the break room into her desktop's USB port. This was not an issue for her since she had used the flash drive plenty of times in the past. She had logged on with her password, and the company's email client was open. This simple act started a chain reaction, launching malware hidden on the flash drive that propagated by attaching a copy of the malignant code to every email she sent. Within hours, the corporate network was thoroughly compromised.

The above hypothetical vignette illustrates an important insight that eludes many Information Technology (IT) managers tasked with cybersecurity: many breaches occur when users are not consciously aware of what they are doing. Also, contrary to recent headlines, not all threats in the cyber realm are malicious in nature. According to a Ponemon study, 70% of US survey respondents and 64% of German respondents stated that more security incidents were caused by unintentional mistakes rather than malicious acts [1]. This is happening in an era when we have clear organizational guidelines pertaining to mandatory Security Education, Training, and Awareness (SETA) programs. We contend that most of these unintentional mistakes are due to habitual behavior that promotes an automatic response. This response may vary based on the experience of individuals.

Previous research supports the idea that automated behavior results from the force of habit [2-4]. It is a given that understanding and linking these automated behaviors more clearly to design features may be highly valuable. But, it is also important to investigate the role a person's experience may play in promoting automated behavior. Can the behavior of a novice and an expert be visualized and compared in a cybersecurity context? This issue needs to be developed for any meaningful modeling and advancement in SETA programs. It is also important to investigate the efficacy of training based on individual groups. Does one-size-fits-all training really work? Interestingly, traditional research in human computer interaction has examined the design and usability components of technology as intended rather than the use/impact cycle [5]. However, by under-emphasizing the use/impact cycle of

URI: https://hdl.handle.net/10125/59929
ISBN: 978-0-9981331-2-6

technology, researchers have predominantly ignored the impact that automated behavior may have.

The purpose of our study was to gauge user behavior by visualizing the brains of users of varied technical experiences in the context of potential phishing attacks. We designed and executed an experiment in which participants were tasked with work-related exercises while being monitored and connected to a suite of neurophysiological tools (e.g., electroencephalography [EEG], eye tracking, and facial encoding of emotion by web camera).

In this paper, we present the results of our pilot study using neurophysiological tools to gain a more complete understanding of human behavior in a work context while individuals interacted with emails covertly staged as a phishing attack. The next section provides the motivation and basis of our argument that unintentional mistakes are due to automated behavior, which may be due to individual differences in experience. We report the results of our EEG analysis and provide examples of the additional neurophysiological data collected. We also present an emergent model that we plan to integrate with what we have already done as part of our future research. Finally, we discuss the implications of incorporating neurophysiological tools into security research to improve SETA programs.

2. Martin-Morich Model of Consumer Behavior Adapted to Cybersecurity

Compelling research from diverse fields including neuroscience, cognitive, social and behavioral psychology, and behavioral economics, reveals that most human behavior is predominantly the result of unconscious mental processes. When a person is in a familiar situation doing repetitive tasks, behavior rapidly becomes automatic, not open to conscious control. This research challenges the conventional wisdom embedded in most models of human behavior that posit humans are rational agents making conscious decisions.

The impact of these research streams to cybersecurity is profound. At the core of all cybersecurity assumptions is that users are capable of following directions that require conscious attention to behaviors performed in highly habitual settings. From this perspective, it seems logical to assume that explaining cybersecurity policies to users should be sufficient to obtain compliance. Yet, a high percentage of cybersecurity breaches are caused by unconscious user behavior, which is immune to all appeals that rely on conscious mind attention and control. Similar to other recent work in IS [6], we propose adapting the Martin-Morich model of consumer behavior (shown in Figure 1) to develop an improved approach to cybersecurity.

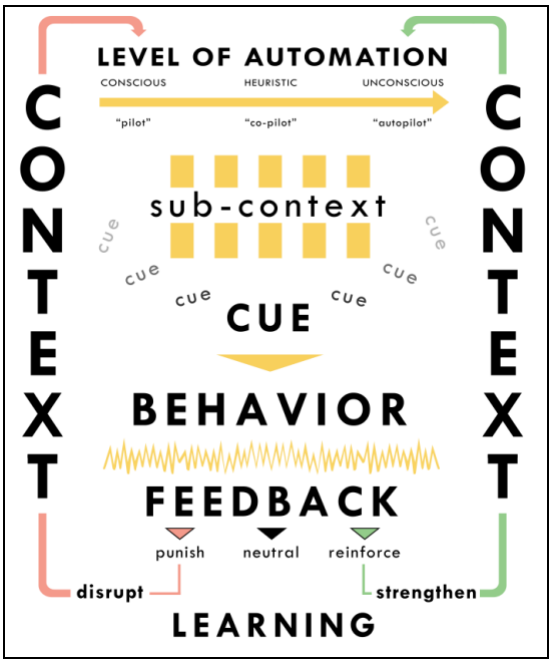


Figure 1: Martin-Morich Model

2.1 The Determinants of Habitual Behavior

Habits are automatic behaviors that are activated by cues in a stable context independent of goals and intentions. They are pre-potent, quick to activate, do not require conscious intervention, and are persistent [7]. The Martin-Morich model posits a dynamic process where the conscious and unconscious minds both participate in guiding decisions and behavior. Decisions and behaviors that are made repeatedly in stable contexts become increasingly habitual. Decisions and behaviors that are novel or occur in situations that are not familiar are more heavily influenced by the conscious mind. The model is designed to more closely reflect real world experiences where habitual behaviors can be disrupted by something that gets the attention of the conscious mind, and even highly complex behaviors can become habitual with sufficient repetitions.

Because the model describes a dynamic process, there is not a clear beginning or end. Behaviors under analysis might be new or ongoing for years. The model is designed to describe the process by which behavior becomes habitual over time and how it is possible to disrupt established habits. In the next few sections we provide an explanation of the tenets of the model.

2.1.1 Level of Automation

Behavior is the culmination of a complex interplay between conscious and unconscious mental processes. The Martin-Morich model places behavior along a continuum of habit formation, with fully conscious behavior (pilot mode) on one end, and completely automatic behavior (autopilot mode) on the other. Between these extremes are heuristics (co-pilot mode) where simple rules govern behavior in familiar situations with multiple plausible behavioral responses. Contrary to human perception, most behavior is generated from the autopilot side of the spectrum [8].

It is important to understand the intensity of the habitual behavior under study to comprehend the risk profile for violating cybersecurity policies and procedures. Behavior that leads to high levels of habituation will inadvertently create greater security risks.

2.1.2 Pilot Mode

Pilot mode describes behaviors that are entirely or largely under the influence of the conscious mind. Pilot mode is engaged in novel situations where established behavioral repertoires do not exist and in situations that are highly important, highly salient, or highly risky.

To engage in conscious thought requires effort, and the conscious mind fatigues rapidly. This is a primary flaw in most security assumptions. There is a pervasive naïve presumption that users will follow security practices if they understand them, and if punishments are in place if they do not. "The defining feature of System 2 (the conscious mind) is that its operations are effortful, and one of its main characteristics is laziness…." [9]. It is this laziness that causes the conscious mind to shift familiar tasks to the unconscious mind as quickly as possible.

A good cybersecurity example of this is passwords. Rules for passwords include not using the same password for multiple accounts and not using easy to remember passwords. In other words, passwords are designed to work against the way the brain works. Predictably, the most frequent calls to IT help lines is forgotten passwords [10]. Due to this reason, employees also have a tendency to share passwords in a team setting [11]. However, that is due to not only the password being difficult to recall, but due to an element of trust that exists as being part of a team [12].

2.1.3 Co-pilot

Co-pilot mode describes behaviors that have been repeated in stable environments but introduce conditional changes. For example, at the grocery store a shopper might develop a heuristic to stock up when a particular item goes on sale. Heuristics are quite common in working with information systems as users develop shortcuts based on varying responses from programs, devices and other users. Most users receive a large volume of emails every day and unconsciously develop heuristics about which emails get responses. For example, an employee may reply to an email in an order that is dependent on who sent it. An urgent email from a supervisor may dictate first response, whereas messages from unidentifiable resources may be deleted. In this scenario, an attacker may assume that an employee has certain heuristics, and therefore may create a message that spoofs a supervisor.

The conscious and unconscious minds work together to solve innumerable tasks throughout the day. Heuristics are simplified decision sets that can be described as the conscious mind intervening minimally to perform an action that is familiar. Heuristics also represent a threat to security because the conscious mind may not be sufficiently engaged to properly understand the security implications of a given behavior. For example, people in buildings that require badges to unlock doors might hold open the door for a woman, an elderly person, or someone with their hands full.

2.1.4 Autopilot

Autopilot mode represents behaviors that are repeated automatically without the need for conscious involvement. The transition from conscious to unconscious action can be seen in learning to type, where the conscious mind is at first heavily taxed, but quickly shifts learning of finger placement to the unconscious. The conscious mind thinks the word, the unconscious mind types. Once learned, the user's typing speed is negatively impacted by the intrusion of the conscious mind, as when a user looks at the keyboard.

Autopilot mode works outside of conscious awareness, and its workings are not available to conscious introspection. This means that a user may perform a behavior unknowingly that violates a policy that they understand and agree with. An example of this is Microsoft's Windows operating system. In attempting to make Windows more secure, the designers forced users to click an "allow" button before tasks that might open up the computer to

intrusion. But the 'allow' button was activated for numerous routine permissions, causing acceptance to become unconscious. This new habit defeats the purpose and effectiveness of this cybersecurity solution.

The unconscious mind works automatically and effortlessly; a user cannot turn it off. This means to a large degree even when someone is consciously interacting with an information system, there is still a significant amount of information being processed by the unconscious mind. Often what the user might describe as a Pilot decision is simply the conscious mind accepting a decision presented by the habitual mind. Moreover, because the conscious mind requires will and effort, it exhausts rapidly. Expecting users to remain consciously vigilant in highly contextualized environments is unrealistic.

Habits form in stable contexts; situations that become familiar through unchanging repetition—like most workspaces. Established contexts signals the conscious brain that it does not have to pay attention; that routines that have worked before can be executed without conscious mind attention. Anyone who works in front of a computer screen for hours at a time, looking at the same programs, the same walls, sitting in the same chair for hours a day forms a uniquely powerful context. This is the central challenge to all efforts at cybersecurity; the very nature of working with PCs and programs puts people in highly habit-forming contexts. Considering that one of the greatest threats an organization faces is from insiders [13], employees in a highly contextualized environment may be so used to sharing their passwords with team mates, that may inadvertently share it with someone who they initially may not have trusted. Password sharing continues to be a serious issue even though security education and training campaigns are carried out by organizations on a regular basis [14].

2.1.5 Cues

Cues are stimuli that have become triggers of habitual behavior in contextualized situations. The human brain is inundated with millions of stimuli, the vast majority of which are not processed by the conscious mind. However, when a behavior becomes closely associated with a context, specific stimuli become cues that trigger that behavior, such as responding instantly to an email. Cues are often built into information systems to create a desired behavior, such as a distinct sound to alert the user that a task needs to be performed. Once users become trained to automatically respond to a cue, they may respond to that cue inappropriately. A common example of this would be to absent-mindedly click on a link [15] that could be a part of a phishing campaign. However, as explained in the autopilot section, it is the unconscious mind that is ultimately making that decision. Vishwanath et al. [16] suggested that habitual patterns of IT interactions with high levels of email load influenced an individual's likelihood of being phished.

2.1.6 Feedback

Feedback is anything that occurs after a behavior has the potential to be viewed as a consequence of that behavior. Outcomes that increase the likelihood that a behavior will be repeated are termed reinforcing. Those that make a behavior less likely to occur are termed punishing. This is how the unconscious mind learns, by associating an act with a result. The closer in time between action and feedback, the more powerful the association [17]. Generally speaking the purpose of security policies is to ensure compliance via a feedback mechanism [18]. Though this technique has worked in the past, in the mobile cloud computing environment cybersecurity compliance continues to be a major concern [19]. Velte et al. [20] specified the ease of working in the cloud computing environment due to a plethora of applications [20]. However, in an organization setting regardless of convenience, security of mobile based cloud applications is a concern [21]. Delays between a request and feedback can be especially problematic as it would impact the user experience and later use of applications. [22]. The role of habit in this setting was highlighted by Venkatesh, et al. [23]) who found that, after 3 months using an IS, the only significant predictor of later use was prior use; other factors were insignificant. It has also been stated that there is a correlation between ease of use of a system and habit formation [24].

3. Testing Environment and Results

We had an opportunity to pilot test our concept in a controlled environment. This section provides a description of the environment and the results.

3.1 Experimental Procedure

We designed a virtual environment for each participant. The participant side incorporated Windows and Linux desktop environments with a web server and a self-contained email system. We also used a separate virtual environment that housed goPhish, which is an open source phishing framework. At no point did the participants interact

with the goPhish environment. Each participant was tasked with certain exercises that were considered to be a part of their work. These tasks included conducting online searches related to work events and reviewing memos about new work policies. Some tasks requested sending related emails to help simulate an employee interacting with their inbox. While those tasks were being carried out, we sent multiple phishing attempts. The first attempt was for a participant to reset their password by providing their existing password. The second focused on them updating their health benefits and logging into a single sign-on system The third email highlighted a merger between their company and another one, whereby requiring some personal information. The fourth and last phishing attempt asked each participant to use their Gmail account to enable access to the new single sign-on system.

Before interacting with the email system, participants underwent an informed consent procedure where they knew their email habits would be monitored using a suite of neurophysiological tools. Then, they were fitted with an electrode cap for recording their brainwaves and participated in calibration of an eye tracker where the first two participants used eye tracking glasses and the second two used a remote eye tracking system, both developed by Tobii (www.tobii.com).

During the participant's interaction with the email system, sixteen channels of EEG were recorded using the research-grade BioSemi Active Two bioamplifier system (http://www.cortechsolutions.com/Products/Physiological-data-acquisition/Systems/ActiveTwo.aspx) connected to a PC. The electrode cap was configured according to the widely used 10-20 system of electrode placement [25]. Active electrodes were placed on the cap to allow for the recording of brain activations down-sampled at 256 Hz using a Common Average Reference (CAR). The sixteen recorded channels were: frontal-polar (Fp1, Fp2), frontal-central (FC3, FCz, FC4), central (C3, Cz, C4), temporal-parietal (TP7, TP8), parietal (P3, Pz, P4), and occipital (O1, Oz, O2).

In addition to EEG and eye tracking data, we also recorded the small muscular movements in the face using a web camera to detect emotion, cursor movements and mouse-clicks, and all audio and video of the interaction through the iMotions software suite for syncing biometric data (www.imotions.com). At the end, participants were given a brief survey to collect basic demographic information and inquire about their risk propensity and computer playfulness. Each session lasted about an hour.

3.2 Sample

We had six participants as summarized in Table 1. There were 3 males and 3 females with an average age of 37 years and all except one with 10-15 or more years of work experience. Participants 1 and 2 worked for over five years within the IT field and were currently working within the field, whereas Participants 3 and 4 were non-IT workers. Participant 3 was working as a leadership and communications coach for undergraduate students, Participant 4 was working as a graduate research assistant in BioChemistry and was a former high school Chemistry teacher, and Participant 5 was an office business manager. Although Participant 6 was the youngest participant, he had relevant IT work experience.

Table 1: Participant Demographics

No.	Gender	Age	Field
1	M	39	IT
2	F	41	IT
3	M	37	Non-IT
4	F	44	Non-IT
5	F	36	Non-IT
6	M	22	IT

These individuals were purposive sampled to represent males and females within a more mature age range from IT and from outside of the IT field and hence arguably less familiar with security protocols. These individuals should not have experienced cognitive decline associated with aging and yet were old enough that their brains had settled into a stable level of myelination indicative of matured brain function. Further, studies have shown that younger individuals are inherently riskier [26], a bias we wished to avoid.

3.3 Results and Discussion

The goPhish dashboard provided us with all information that the participants were entering in their virtual environment. Figure 2 provides an overview of the results for Participant 1. As the figure shows, we were able to track if a participant not only opened an email, but also if they clicked any of the links, or submitted any data.

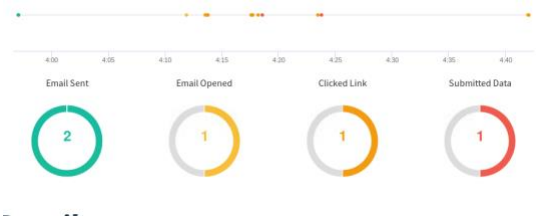


Figure 2: Participant 1

It was interesting to note that even though they had expertise in IT, Participants 1 and 2 fell for all phishing campaigns. Participant 3 as the figure below shows, opened the emails, but did not click any of the links, nor did he provide any information. We later discovered that he had just conducted his annual security training within two weeks of participation; the training was still salient in his mind of what were legitimate emails and not, indicated by statements such as, "Trying to get me to go to my personal Gmail... That dog won't hunt!" and with further reflection, "Corporate wanting me to go to Gmail was really sketchy."

P03 - Financial Info Update	June 6th 2018, 11:50:02 am	2	1	0	0
P03 - Merger	June 6th 2018, 11:49:02 am	2	1	0	0
P03 - Health Benefits	June 6th 2018, 11:48:38 am	2	1	0	0
P03 - Password Reset	June 6th 2018, 11:48:08 am	2	1	0	0

Figure 3: Participant 3

Participant 4 on the other hand as the figure shows, did click on all the links that were part of the phishing campaign and provided information for the password reset and financial information update. She seemed to sense things were going awry for her behavior saying at the end, "I'm sorta feeling like this guy at the end, a sucker [emphasized with laughter]."

Name	Created Date				
P04 - Financial Info Update	June 6th 2018, 3:57:01 pm	2	1	1	1
P04 - Merger	June 6th 2018, 3:56:35 pm	2	1	1	0
P04 - Health Benefits	June 6th 2018, 3:56:15 pm	2	1	1	0
P04 - Password Reset	June 6th 2018, 3:55:39 pm	2	1	1	1

Figure 4: Participant 4

Figures 5 and 6 reflect the actions of our final two participants.

Name	Created Date				
P05-Password Reset	September 12th 2018, 12:38:52 pm	2	1	0	0
P05-Health Benefits	September 12th 2018, 12:38:09 pm	2	1	0	0
P05-Merger	September 12th 2018, 12:37:26 pm	2	1	0	0
P05-Financial Info Update	September 12th 2018, 12:35:54 pm	2	1	0	0

Figure 5: Participant 5

Name	Created Date				
P06-Financial Info Update	September 12th 2018, 2:03:35 pm	2	1	1	1
P06-Password Reset	September 12th 2018, 2:05:20 pm	2	1	1	0
P06-Health Benefits	September 12th 2018, 2:04:14 pm	2	1	0	0
P06-Merger	September 12th 2018, 2:04:07 pm	2	1	1	0

Figure 6: Participant 6

Participant 5 as the Figure above shows, did not click on any of the phishing attempts, where as our final participant did fall for the financial information gathering phishing attempt.

Recordings from the sixteen channels of scalp electrodes were analyzed offline using a previously-validated technique for brain localization and associated software: standardized low resolution brain electromagnetic tomography (sLORETA) [27]. This analysis was conducted for each of the six participants. Figure 5 presents topological plots of neural activations across participants' scalps analyzed for the duration of their activity. These activations are presented on a fixed scale such that brighter areas with yellow indicate highest levels of activation. For each grouping of topological plots, the image on the top row in the center is a back-end view of the brain whereas the image on the bottom row in the center is a front-on view of the brain (with the view indicated in small font in the bottom right corner). Among other things, higher activation in the left hemisphere may indicate stronger positive approach to the activity whereas higher activation in the right hemisphere may indicate negative approach to the activity [28].

The topological plots are all rather different with the exception of Participants 1 and 4 with greatest activation in their prefrontal cortex, an area that has been associated with decision making and planning complex behaviors. Yet these participants are rather different in individual characteristics. Participant 1 is male with many years of IT experience and familiar with virtual environments and security procedures, and Participant 4 is female and self-described as non-

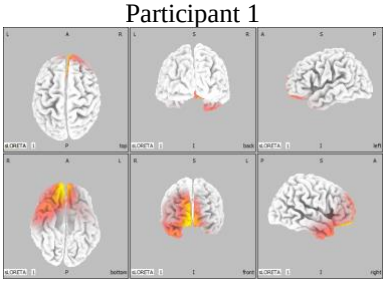
astute with technology. The cognitive difference between these individuals is that Participant 1 shows greater activity on the right hemisphere of his frontal lobe indicating conscious thinking about his actions and judgement of the activities while perhaps reflecting the frustration he felt with the technical environment and its slow performance. Participant 4 may also have this conscious-level of thinking about the activity but she was laughing at herself throughout and this degree of self-amusement may be the slight hemispheric difference shown favoring the left hemisphere.

Participant 2 had greatest activation in her occipital lobe associated with visual processing. She made statements like, "I just could look at my inbox and see that I didn't need to click on any of those emails." Unfortunately, this statement is not in line with her actions as she did in fact click on them. This is where analysis of her qualitative statements may point to her clicking on emails to verify her notions rather than actually falling for the campaign which would be indicated by her dashboard report. The lack of frontal lobe activity may indicate the neural efficiency of an expert as her role is to educate and secure networks at her job. Further, a positive approach to the activity is indicated by greater activation in the left hemisphere and was reinforced by her smiling through the activity.

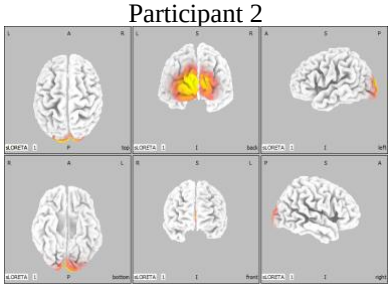
The EEG results of Participant 3 are interesting in the context of the study because the greatest activation appears in the superior frontal gyrus of the frontal lobe, an area associated with higher cognitive functions such as working memory. It is possible that his brain topography is a reflection of him trying to recall what he was typing in an email because the system crashed on him while he was composing emails before he had an opportunity to save them as drafts which he verbalized to researchers.

Participants 5 and 6 had greatest activation in their frontal lobe but in different areas; Participant 5 had greatest activation in her inferior temporal gyrus (a.k.a. the IT cortex but not because of an association with information technology) whereas Participant 6 had greatest activation in his middle frontal gyrus. The IT cortex is associated with processing visual stimuli and matching of color and form. This participant seemed to be more engrossed with a particular task to identify t-shirts for a work function. Contrastingly, the middle frontal gyrus is associated with attention. Particularly, the right middle frontal gyrus, as is highlighted for Participant 6, has been tied to numeracy or the ability to conduct numerical operations [29]. Here we may be seeing evidence of this participant's difficulty in keeping track of which task he was on as he was observed repeatedly shuffling the task papers and verifying that he had conducted the earlier tasks.

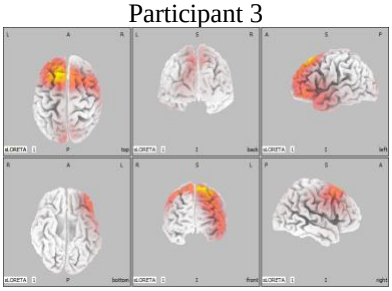
Participant 1



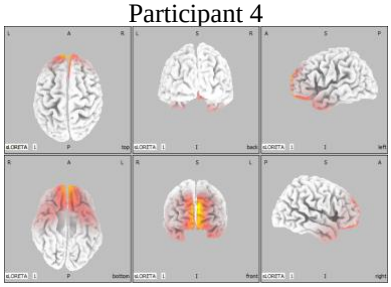
Participant 2



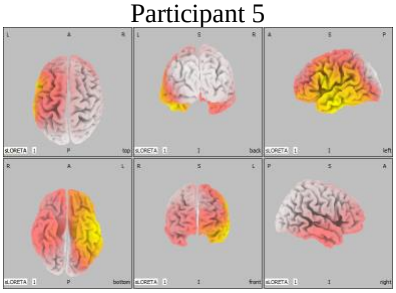
Participant 3



Participant 4



Participant 5



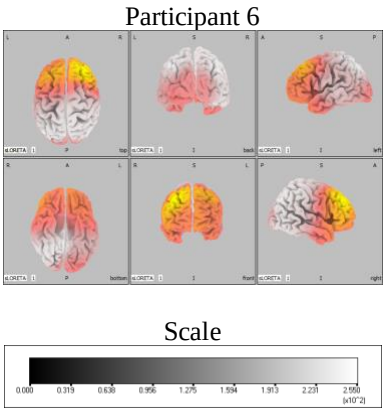


Figure 5: Topological Plots of EEG Activations for Participants

Figure 6 illustrates results that may be obtained from eye tracking to generate heatmaps of a participant's attention. These heatmaps show similar patterns for Participants 1 and 2 scanning the Inbox with their eyes and yet this contrasts with how they were mentally processing the experience. Further, eye tracking allows us to confirm engagement with the interface. In addition to EEG and eye tracking data, we were able to obtain stimulus-synced assessments of emotion ranging from joy to anger based on facial encoding of slight muscular movements recorded by web camera. We do not report here the results of these additionally-edifying measures to instead focus on the richness that EEG may provide to a study.

Figure 6: Heatmaps Generated from Eye Tracking Data of Participants 1 (left) and 2 (right) Viewing the Email Inbox

Further reflection indicates that EEG may be triangulated with emotion, eye tracking, screen capture, survey, and qualitative debrief to more fully understand a person's experience while engaging with a phishing campaign. Context of the session, individual characteristics, and personal account of mental processing are all necessary to better understand such varied results as may be obtained using biometric tools. This variation in human mental processing is illustrated by the brain activations of the six participants who themselves vary. Yet we may better understand the impact of SETA programs with these tools providing richer insights to their thought processes and behavior. With further study, we may see trends across individual characteristics and experiences and better target interventions.

3.4 Participant Survey

Experiment participants completed a short survey, which asked them about their general risk perceptions, computer playfulness, and specific risk perception.

For general risk perceptions, participants were asked to indicate 1, 2 or 3 where 1=During most of my life, I found dangerous or risky situations exhilarating and was willing to give up some control for the thrill. 2=During most of my life, I found some danger or risk exciting, but only if I had control of the situation. 3=During most of my life, I have avoided risky situations because I believe that it is better to be safe than sorry. The mean for pilot participants was 2.5.

Computer playfulness was measured using a 1-7 Likert style scale where 1 represents Not at All and 7 represents All the Way. The questions asked participants how they would characterize themselves when they use microcomputers. When presented with specific adjectives, they chose 1-7 to match the description of themselves when interacting with microcomputers. Table 2 shows the Mean for the responses.

Table 2: Computer Playfulness Response Means

Adjective	Mean
Spontaneous	3.25
Unimaginative	3.75
Flexible	6.25
Creative	5.25
Playful	4.5
Unoriginal	3.25
Uninventive	3.25

Finally, participants were asked to indicate one of the following measures of specific risk that we developed to measure risk perception in this study. 1=I believe that the overall riskiness of the Email system is very high. 2=I believe that the overall riskiness of the Email system is very low. The mean for participants was 1.5.

4. The Maturation of our Model Toward a Specific Training Platform

There is an emergent model out of this research that is shown in Figure 7. The model is based on the following premise. As mentioned earlier, the key dependent variable of interest is the actual behavior of the individual. Here the actual behavior relates to whether an individual fell for a phishing attack or not. Based on our research and literature, we argue for the following model. The model is shown as an input-process-output model.

The key inputs into the model are the actual work task being performed by an individual, which in our case was answering office emails. The actual work task relates to individual performance. The task complexity in this case would be rated as medium. The threat is as it relates to the anomaly in the individual's task that may result in an information security breach. In the case of our study, this related to the phishing attempt designed by the researcher.

As individuals went through the process of doing their tasks, two key variables that influenced actions were the risk perception of an individual and the cognitive load experienced by the individual. The neuroscience-based approach illustrated in this paper suggests that there may be a difference between how people act and what is going on in their minds. Based on this research, we suggest the following propositions:

P1: The greater the novelty of the threat, the greater the risk perception of the task.

P2: The more complicated the task, the more cognitive load it presents.

P3: The greater the risk perception, the greater the likelihood the individual's actions will be secure.

P4: The greater the cognitive load, the less likely the actions of an individual will be secure.

More broadly, the emergent model argues that the focus of security training needs to incorporate both the threat novelty and task complexity. Those are the key determinants of cognitive load that in turn lead to secure behavioral actions.

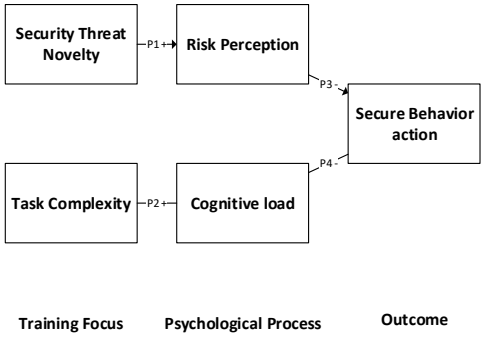


Figure 7: Emergent Model

5. Conclusion

Email is still one of the most widely used tools in the workforce to communicate and collaborate. Hence it is crucial that employees know how to identify and avoid phishing emails as the best way to thwart a phishing attack. The pilot test presented here, simulated an aspect of a regular day at the office to see what a person experienced while interacting with their email inbox and working through tasks, how their brain was affected, and the emotions experienced. Neurophysiological tools helped illustrate the thought processes behind participants' statements and actions; combined with consideration of individual characteristics, these tools may help shed more light on human behavior. Getting a full view of the lived experience of a person during a phishing attack may prove helpful in advancing the effectiveness of SETA programs. This study seems to give credence to the notion that proximity of training to engagement with a phishing campaign may have the most influence on the level of awareness and success that a person has in successfully resisting a phishing campaign. In future work, we will expand the testing environment to incorporate the emergent model presented here and expand the sample population to industry professionals with a range of IT and non-IT experience.

6. Acknowledgments

We would like to thank Matt Freemyer for his work to run the pilot study in the BrainLAB. This work was supported by a faculty fellowship made possible by SunTrust. We would also like to thank

7. References

[1] Ponemon. (2015, September 15). *The Unintentional Insider Risk in United States and German*

Organizations. Available: http://www.raytheoncyber.com/spotlight/ponemon/pdfs/3P-Report-UnintentionalInsiderResearchReport-Ponemon.pdf

[2] S. S. Kim, N. K. Malhotra, and S. Narasimhan, "Research note—two competing perspectives on automatic use: A theoretical and empirical comparison," *Information Systems Research*, vol. 16, no. 4, pp. 418-432, 2005.

[3] J. Jasperson, P. E. Carter, and R. W. Zmud, "A Comprehensive Conceputalization of the Post-Adoptive Behaviors Associated with IT-Enabled Work Systems," *MIS Quarterly*, vol. 29, no. 3, p. 15, 2005.

[4] J. A. Ouellette and W. Wood, "Habit and intention in everyday life: the multiple processes by which past behavior predicts future behavior," *Psychological bulletin*, vol. 124, no. 1, pp. 54-74, 1998.

[5] P. Zhang and N. Li, "The intellectual development of Human-Computer Interaction research: A critical assessment of the MIS literature (1990-2002)," *Journal of the Association for information Systems*, vol. 6, no. 11, pp. 227-292, 2005.

[6] H. Zafar, A. B. Randolph, and N. Martin, "Toward a more secure HRIS: The role of HCI and unconscious behavior," *AIS Transactions on Human-Computer Interaction*, vol. 9, no. 1, pp. 59-74, 2017.

[7] W. Wood and D. T. Neal, "The habitual consumer," *Journal of Consumer Psychology*, vol. 19, no. 4, pp. 579-592, 2009.

[8] B. Verplanken, V. Myrbakk, and E. Rudi, "The measurement of habit," in *The routines of decision making*, T. Betsch and S. Haberstroh, Eds. NJ, 2005, pp. 231-247.

[9] D. Kahneman, *Thinking, fast and slow*. New York: Macmillan, 2011, p. 533.

[10] R. Witty and K. Brittain, "Automated password reset can cut IT service desk costs," *Gartner Report*, 2004.

[11] E. Grosse and M. Upadhyay, "Authentication at scale," *Security & Privacy, IEEE*, vol. 11, no. 1, pp. 15-22, 2013.

[12] M. A. Sasse, S. Brostoff, and D. Weirich, "Transforming the 'weakest link'—a human/computer interaction approach to usable and effective security," *BT technology journal*, vol. 19, no. 3, pp. 122-131, 2001.

[13] M. Warkentin and R. Willison, "Behavioral and policy issues in information systems security: the insider threat," *European Journal of Information Systems*, vol. 18, no. 2, pp. 101-105, 2009.

[14] M. Whitty, J. Doodson, S. Creese, and D. Hodges, "Individual Differences in Cyber Security Behaviors: An Examination of Who Is Sharing Passwords," *Cyberpsychology, Behavior, and Social Networking*, vol. 18, no. 1, pp. 3-7, 2015.

[15] Z. Benenson, G. Lenzini, D. Oliveira, S. Parkin, and S. Uebelacker, "Maybe Poor Johnny Really Cannot Encrypt-The Case for a Complexity Theory for Usable Security," in *Proc. of the New Security Paradigm Workshop*, 2015.

[16] A. Vishwanath, T. Herath, R. Chen, J. Wang, and H. R. Rao, "Why do people get phished? Testing individual differences in phishing vulnerability within an integrated, information processing model," *Decision Support Systems*, vol. 51, no. 3, pp. 576-586, 2011.

[17] E. Kandel, *In search of memory*. Oregon Health and Science University, 2008.

[18] M. Warkentin, A. C. Johnston, and J. Shropshire, "The influence of the informal social learning environment on information privacy policy compliance efficacy and intention," *European Journal of Information Systems*, vol. 20, no. 3, pp. 267-284, 2011.

[19] L. M. Kaufman, "Data security in the world of cloud computing," *Security & Privacy, IEEE*, vol. 7, no. 4, pp. 61-64, 2009.

[20] T. Velte, A. Velte, and R. Elsenpeter, *Cloud computing, a practical approach*. NY: McGraw-Hill, Inc., 2009.

[21] J. W. Rittinghouse and J. F. Ransome, *Cloud computing: implementation, management, and security*. UK: CRC press, 2009.

[22] J. Y. Tsai, P. Kelley, P. Drielsma, L. F. Cranor, J. Hong, and N. Sadeh, "Who's viewed you?: the impact of feedback in a mobile location-sharing application," in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, California, US, 2009, pp. 47-58: ACM.

[23] V. Venkatesh, M. G. Morris, and P. L. Ackerman, "A longitudinal field investigation of gender differences in individual technology adoption decision-making processes," *Organizational behavior and human decision processes*, vol. 83, no. 1, pp. 33-60, 2000.

[24] A. Burton-Jones and G. S. Hubona, "The mediation of external variables in the technology acceptance model," *Information & Management*, vol. 43, no. 6, pp. 706-717, 2006.

[25] R. W. Homan, J. Herman, and P. Purdy, "Cerebral location of international 10–20 system electrode placement," *Electroencephalography and Clinical Neurophysiology*, vol. 66, no. 4, pp. 376-382, April 1987.

[26] L. P. Spear, "The adolescent brain and age-related behavioral manifestations," *Neuroscience & Biobehavioral Reviews*, vol. 24, no. 4, pp. 417-463, 2000.

[27] R. D. Pascual-Marqui, "Standardized low-resolution brain electromagnetic tomography (sLORETA): technical details," *Methods Find Exp Clin Pharmacol*, vol. 24, no. Suppl D, pp. 5-12, 2002.

[28] R. J. Davidson, "Anterior Cerebral Asymmetry and the Nature of Emotion," *Brain and Cognition*, vol. 20, pp. 125-151, 1992.

[29] M. S. Koyama, D. O'Connor, Z. Shehzad, and M. P. J. S. r. Milham, "Differential contributions of the middle frontal gyrus functional connectivity to literacy and numeracy," vol. 7, no. 1, p. 17548, 2017.