Towards An Assessment of Audio, Visual, and Haptic Alerts and Warnings to Mitigate Risk of Phishing Emails Susceptibility

Presented by
Yair Levy and Molly Cooper

College of Computing and Engineering
NOVA SOUTHEASTERN UNIVERSITY
NSU Florida

FERRIS STATE UNIVERSITY

http://CyLab.nova.edu/

Our Speakers For Today's Webinar

Dr. Yair Levy
Professor of I.S,
Nova Southeastern University

Yair Levy, Ph.D. is a Professor of IS and Cybersecurity at Nova Southeastern University (NSU), the Director of the Center for Information Protection, Education, and Research (CIPhER), and chair of the Cybersecurity Faculty Group at the college. During the mid to late 1990s, Dr. Levy assisted NASA to develop e-learning platforms as well as manage Internet and Web infrastructures. He authored numerous peer-review publications and his publications were cited over 4200 times.

He is frequently invited as a Subject Matter Expert (SME) on cybersecurity topics to provide keynote talks at national and international meetings, as well as regular media interviews in print, radio, and TV. He holds a BS.c. in Aerospace Engineering (Technion), MBA and Ph.D. in Management Information Systems from Florida International University.

Our Speakers For Today's Webinar

Molly Cooper
Assistant Professor of I.S,
Ferris State University

Molly Cooper is an Assistant Professor for Information Security and Intelligence at Ferris State University, and former GRC (Governance, Risk, and Compliance) Lead at Michigan State University (MSU). Professor Cooper has created several compliance programs ensuring the security of payment card data, security control compliance, and healthcare data.

Her primary technical and research interests are information security controls, gamification of cybersecurity concepts, IT risk, IT compliance, and phishing prevention. She holds both undergraduate and graduate degrees in information security and project management, and is currently pursuing a Ph.D. in information assurance

Learning Objectives (LOs)

At the end of this workshop, the participants will:

- Learn the concept of Human-Centric Lens in Cybersecurity
- Learn about the theoretical concepts behind human factors in cyber
- Understand the differences between System 1 and System 2 thinking
- Introduce to the research topics related to:
  - Cybersecurity skills of non-IT professionals
  - An Examination of User Detection of Business Email Compromise Amongst Corporate Professionals
  - Cyber situational awareness and curiosity as indication of risk
  - Assessing the impact of human error types on large data breaches
  - Cognitive load and its impact on password strength
  - Experimental Study to Assess the Role of Environment and Device Type on the Success of Social Engineering Attacks
- Learn about an new innovative assessment of audio, visual, and haptic alerts and warnings to mitigate risk of phishing emails susceptibility

LEVY CyLAB

The research in our laboratory focuses on the ***human-centric*** lens of all three cybersecurity pillars with increased emphasis on addressing the following four key research areas and their interconnections: Cybersecurity threat mitigation, Social-Engineering, User-authentication, and Privacy

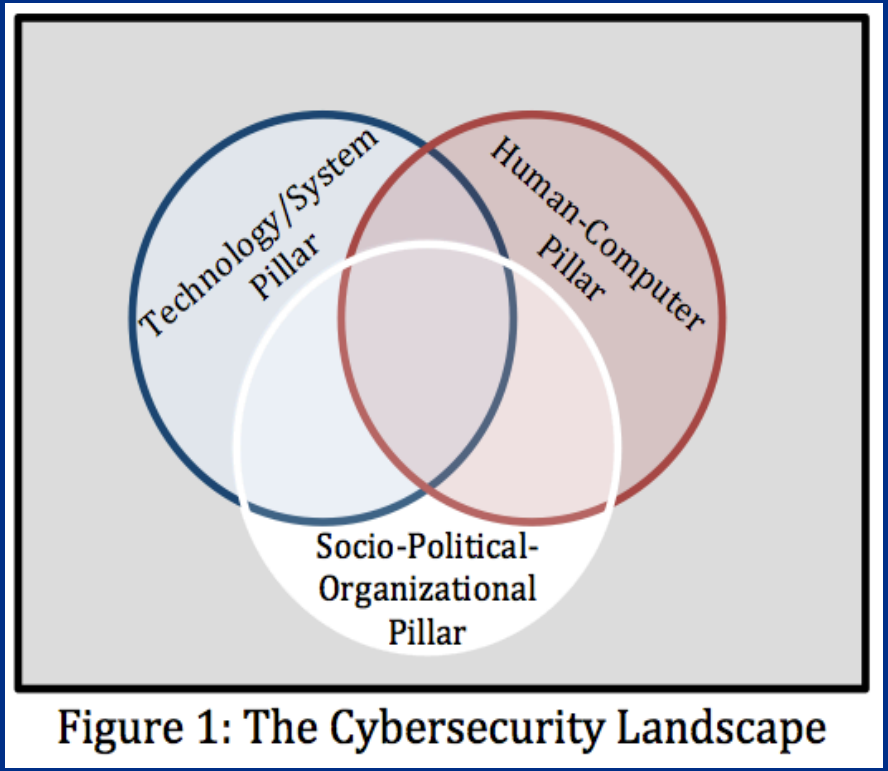
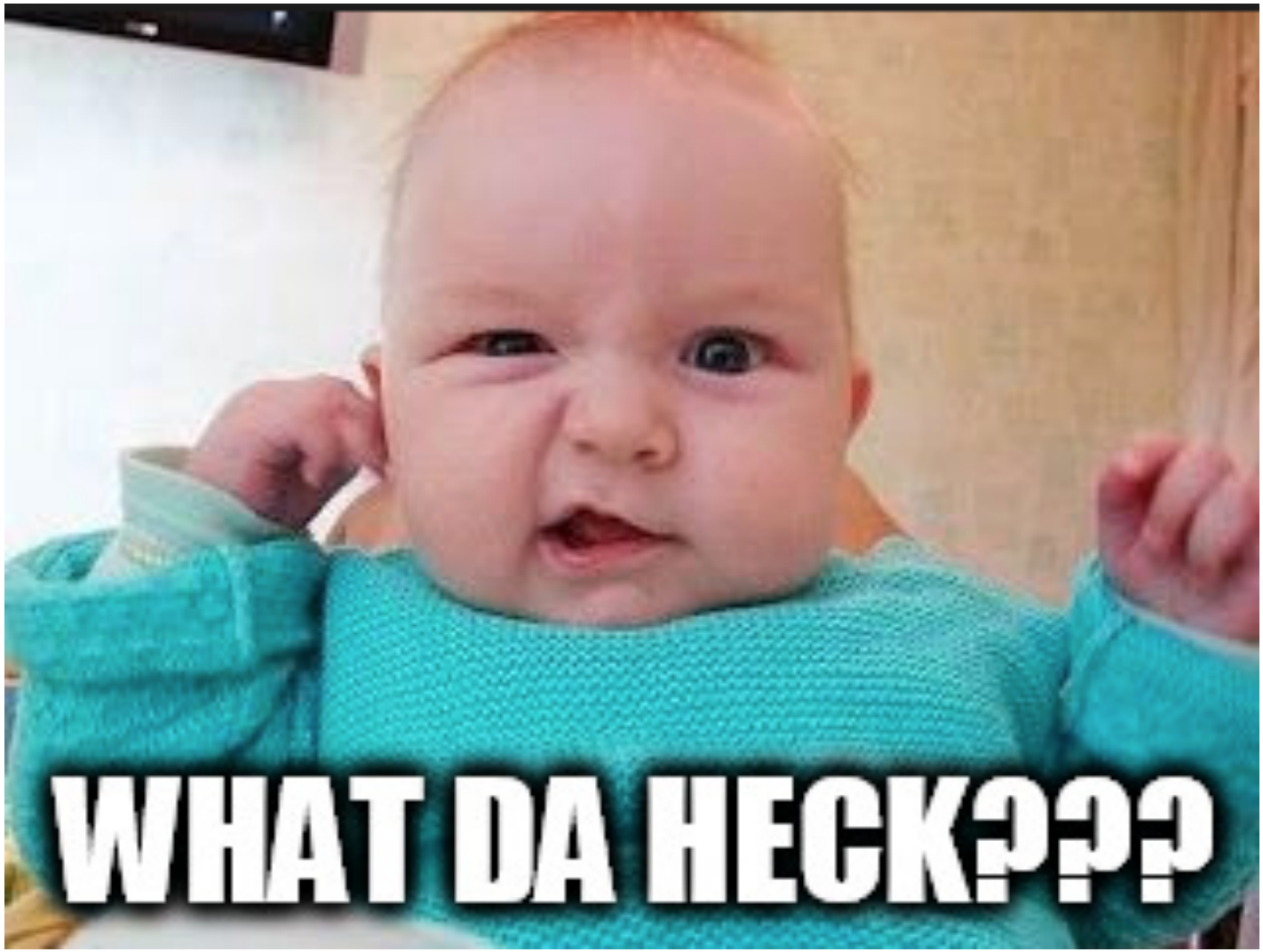


Figure 1: The Cybersecurity Landscape

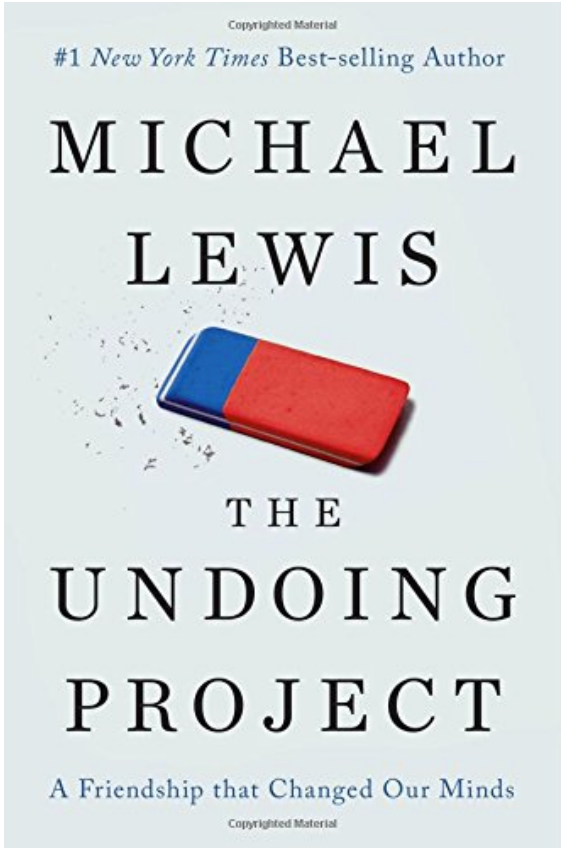
http://CyLab.nova.edu/

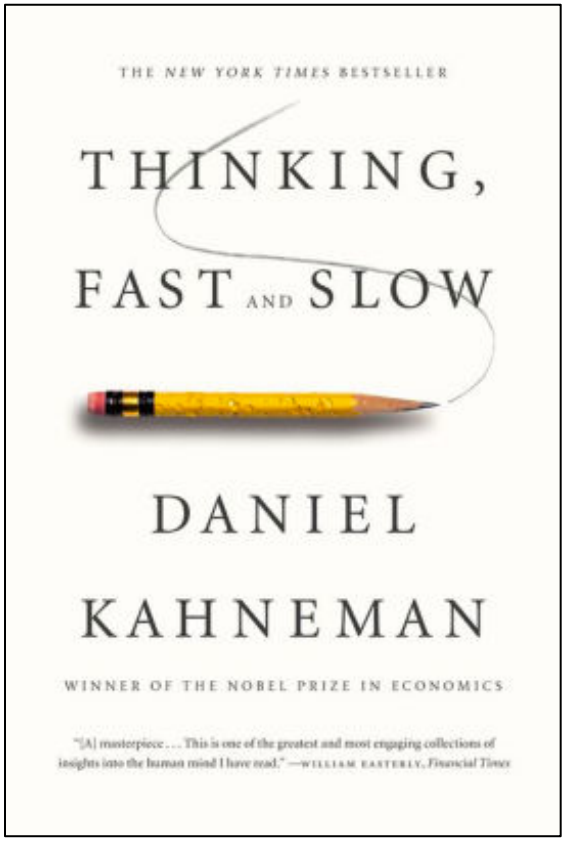
NSU Florida

Human-Centric “lens” of Cybersecurity?



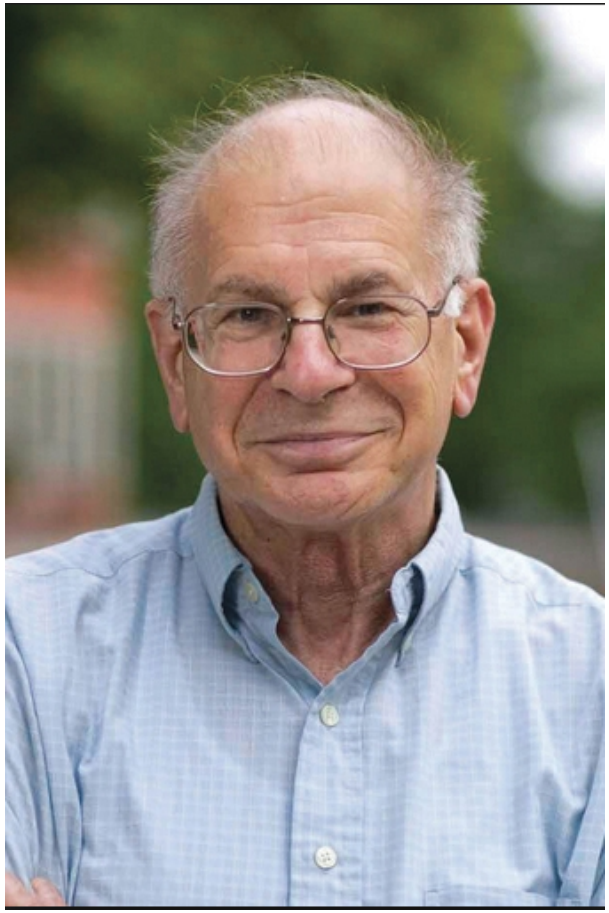
Some Theoretical Concepts:

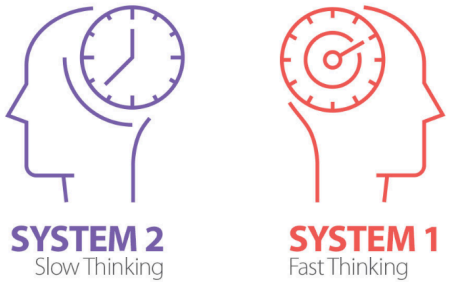




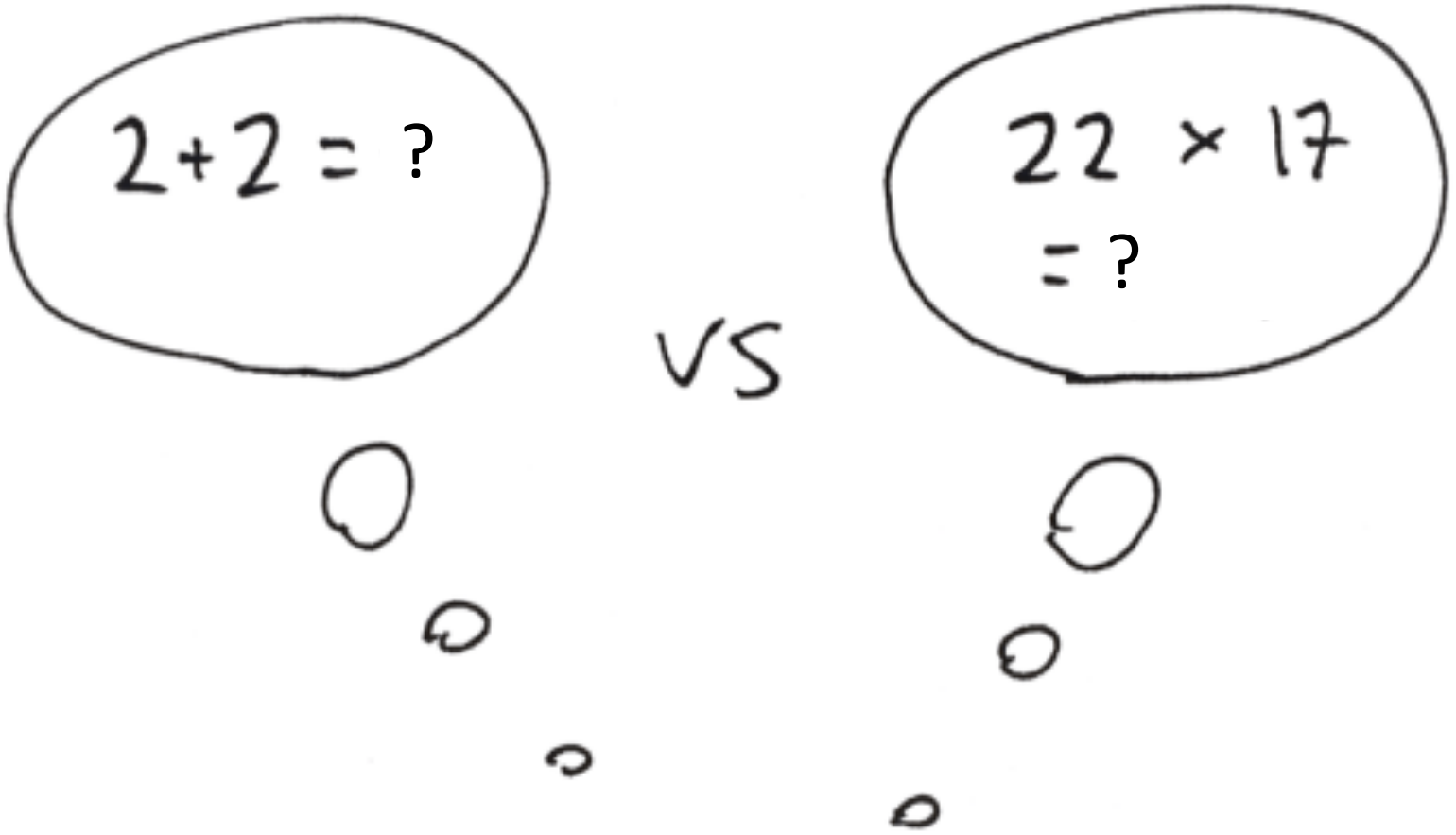
Dr. Daniel Kahneman

An Israeli-American psychologist notable for his work on the psychology of judgment and decision-making, as well as behavioral economics, for which he was awarded the **2002 Nobel Prize in Economic Sciences** (shared with Vernon L. Smith). His empirical findings challenge the assumption of human rationality prevailing in modern economic theory. With **Amos Tversky** and others, Kahneman established a cognitive basis for common human errors that arise from heuristics and biases.

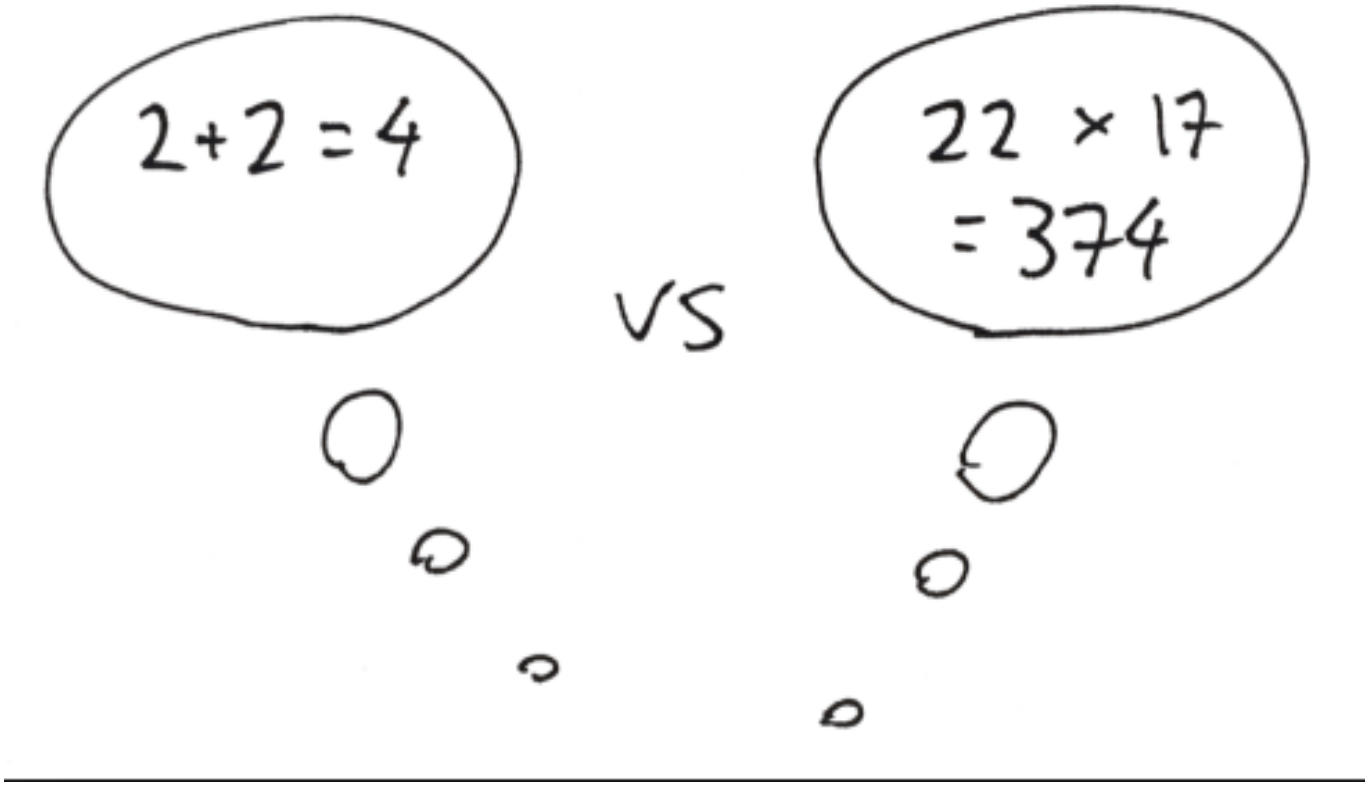




Quick – Solve **One** of These!



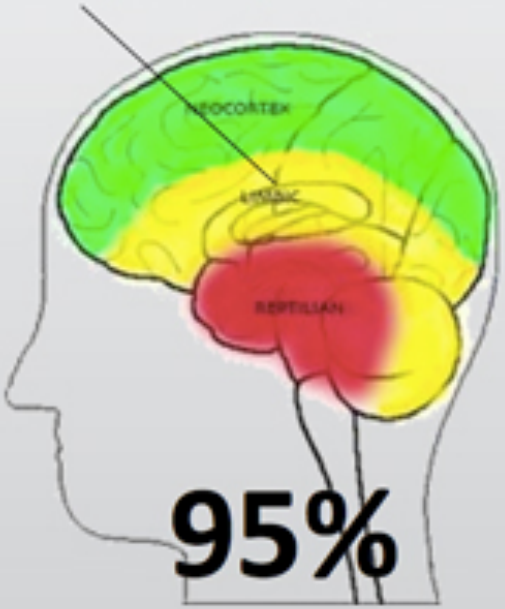
Our Brain Works on Auto-Pilot Sometimes…



SYSTEM 1 AND SYSTEM 2 PROCESSING

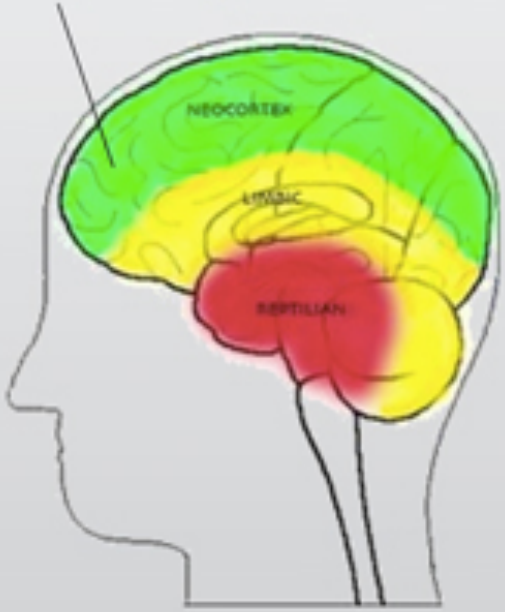
"FIRST REACTIONS"

System 1 ≈ fast, automatic, impulsive, associative, **emotional**, and unconscious processing ≈ limbic.

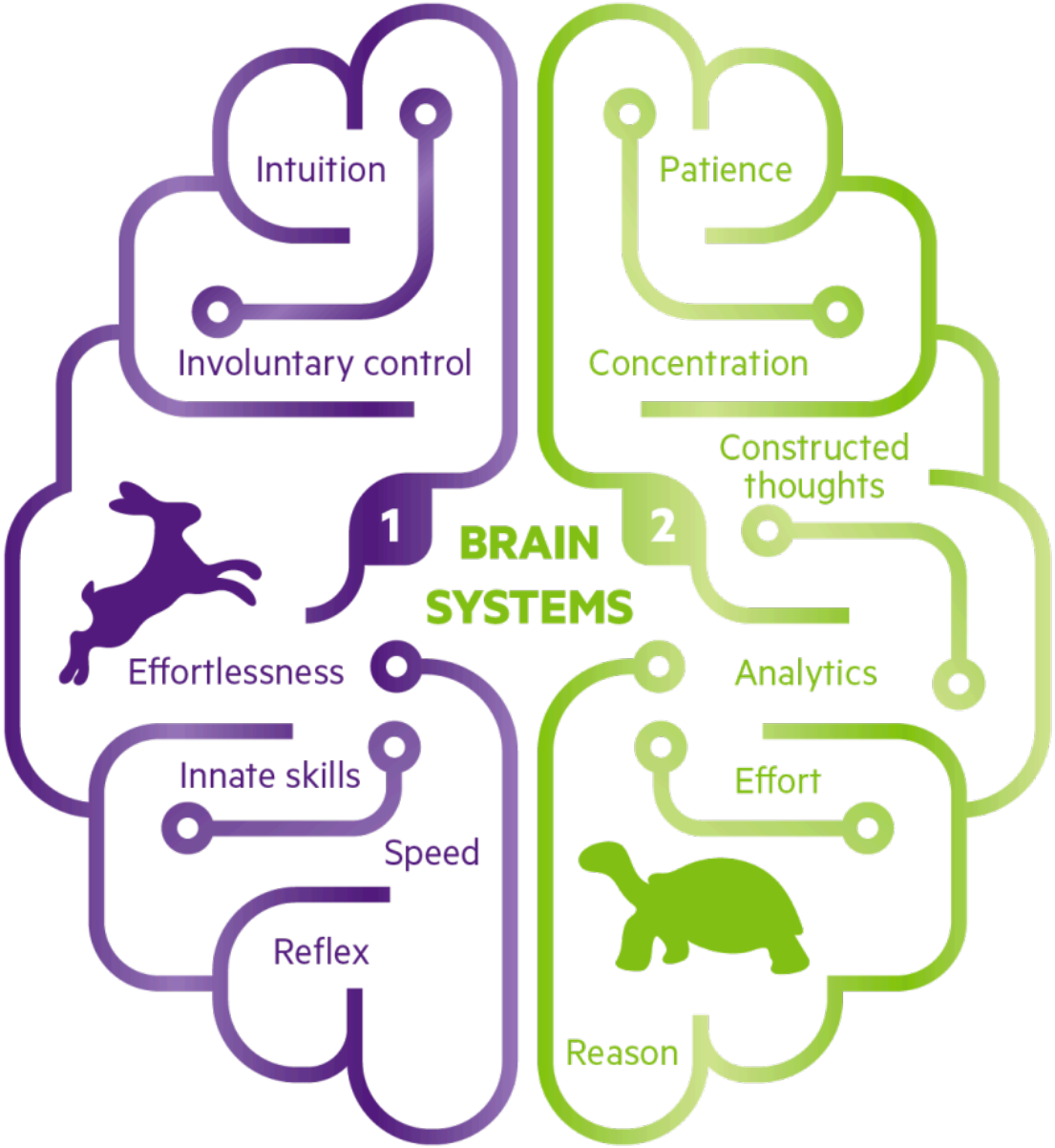


"THINKING"

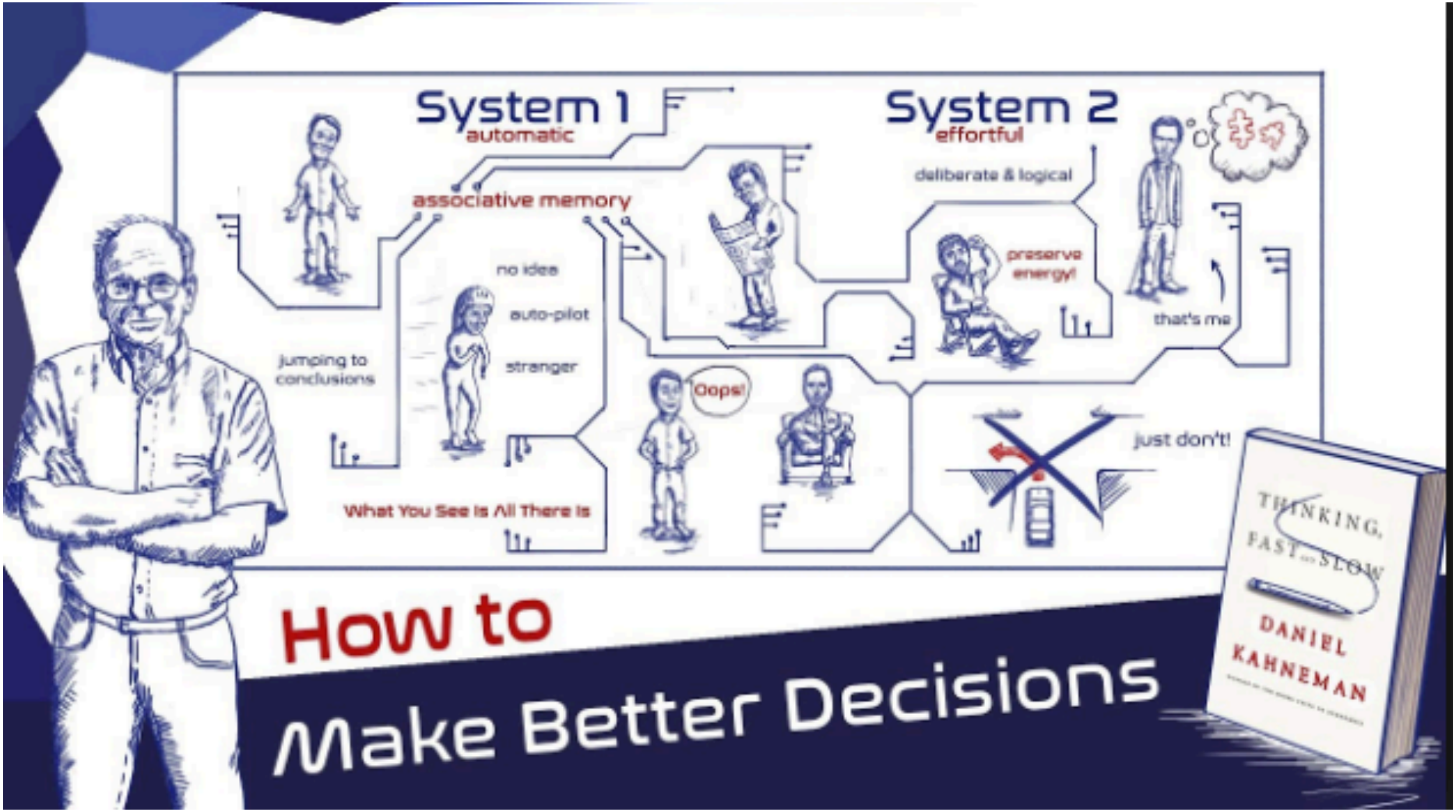
System 2 ≈ slower, conscious, reflective, deliberative, analytical, rational, logical processing ≈ neocortex.



System 1 vs. System 2 Thinking



System 1 vs. System 2 Thinking



Skill Development and Competencies

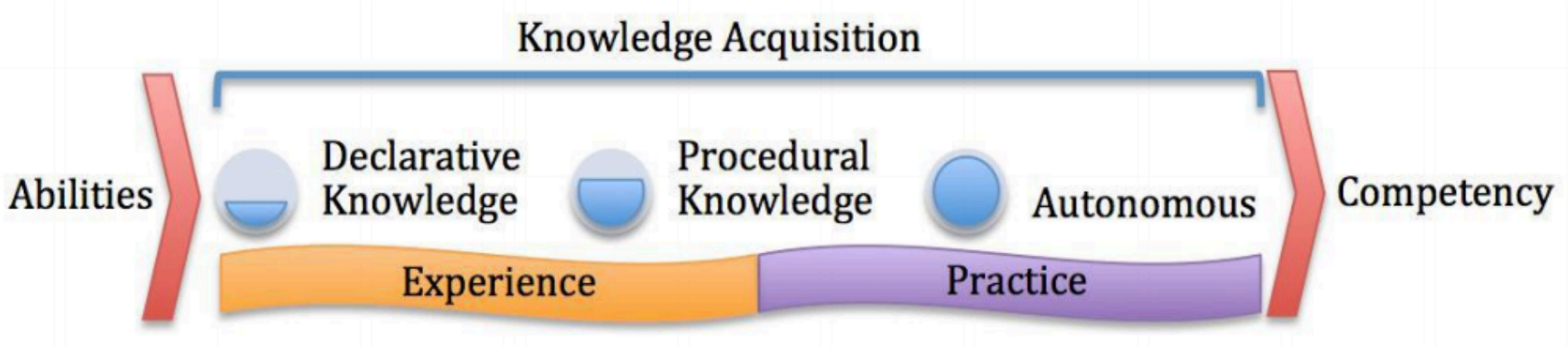
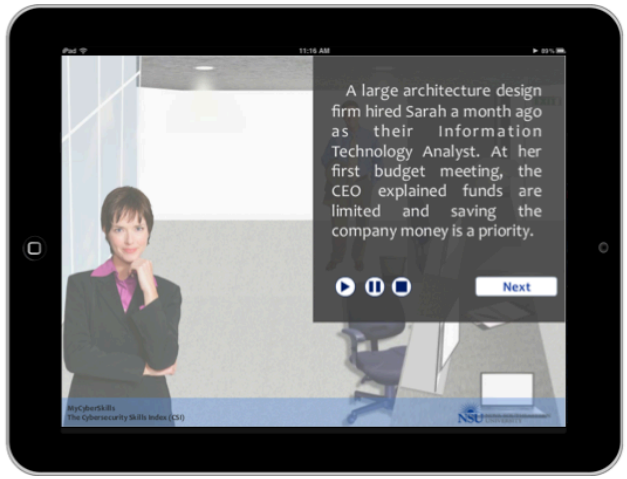


Figure 1. The Stages of Skill Development and Competency Attainment

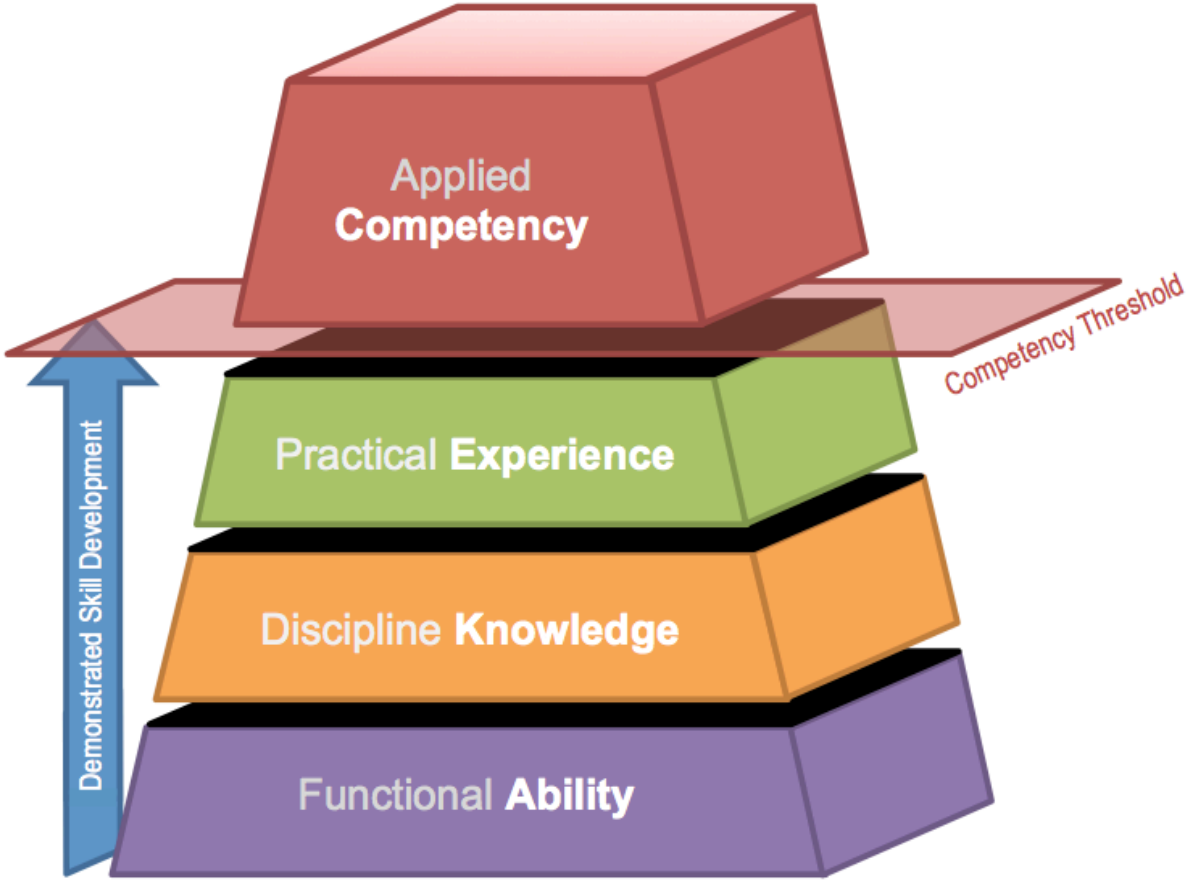
Carlton, M., & Levy, Y. (2017). Cybersecurity skills: The cornerstone of advanced persistent threats (APTs) mitigation. *Online Journal of Applied Knowledge Management (OJAKM), 5*(2), 16-28. Retrieved from: https://www.iiakm.org/ojakm/articles/2017/volume5_2/OJAKM_Volume5_2pp16-28.pdf

Measuring Cybersecurity Skills



Melissa Carlton, Ph.D. - Huston Buptist University - Assistant Professor
Dissertation title (2016): *"Development of a cybersecurity skills index: A scenarios-based, hands-on measure of non-IT professionals' cybersecurity skills"*

Measuring Cybersecurity Competency

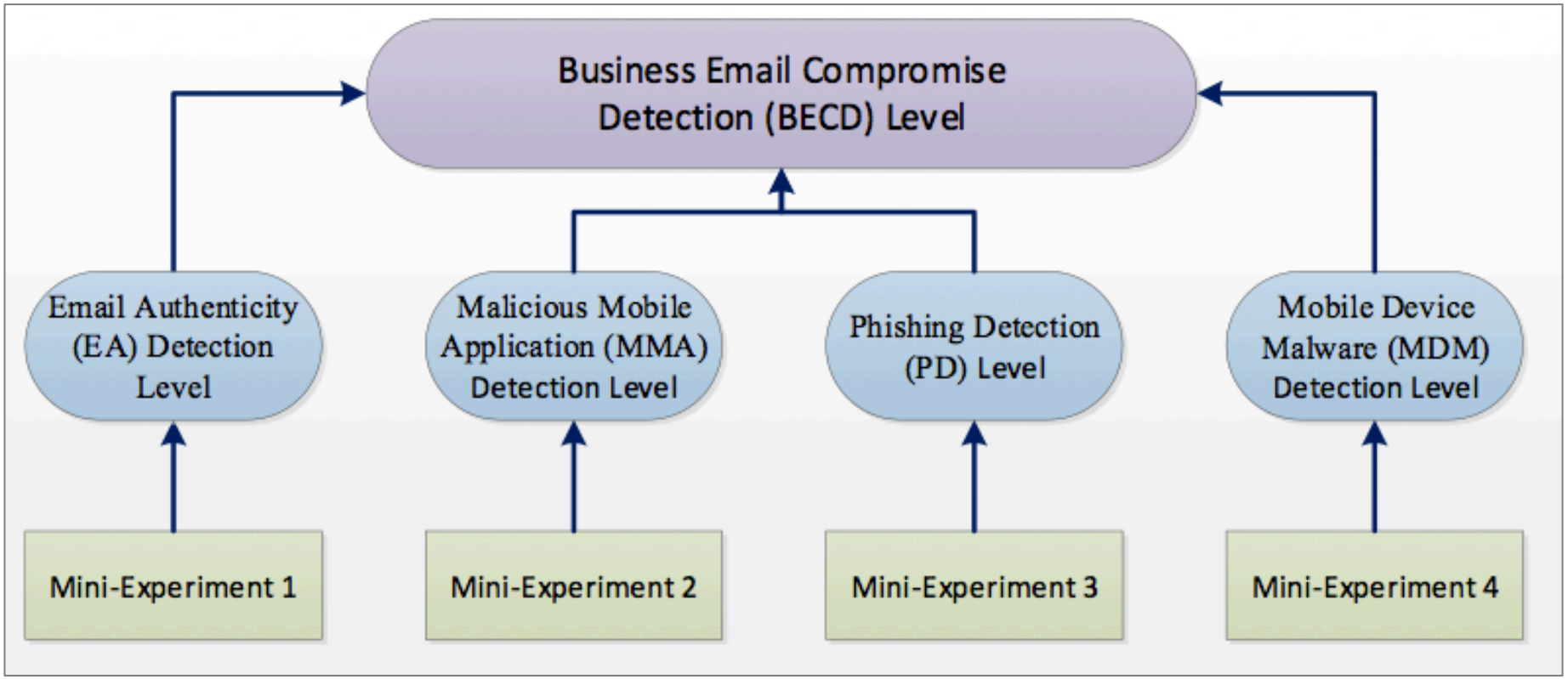


Richard Nilsen, Ph.D. - DoD and Middle Georgia State University

Dissertation title (2017): "*Measuring Cybersecurity Competency: An Exploratory Investigation of the Cybersecurity Knowledge, Skills, and Abilities Necessary for Organizational Network Access Privileges*"

Detecting Business E-mail Compromise (BEC)

http://becd.app/



Shahar (Sean) Aviv, Ph.D. - ExcelNet.com

Dissertation title (2019): *"An Examination of User Detection of Business Email Compromise Amongst Corporate Professionals"*

Cyber Situational vs. Curiosity as Measure of Risk

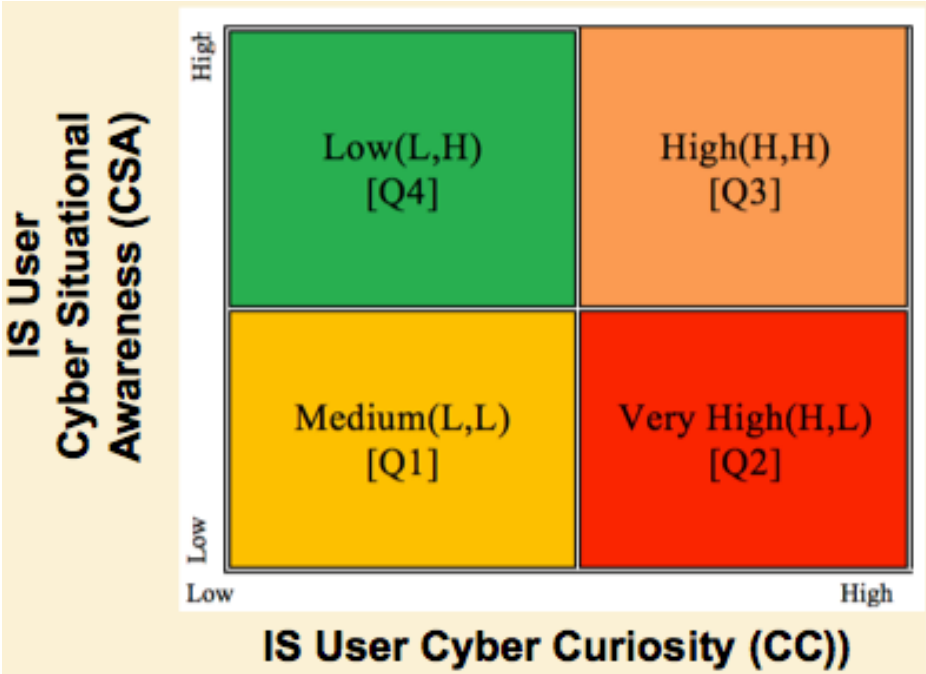


Figure 3 User cyber SA and cyber curiosity cyber risk taxonomy

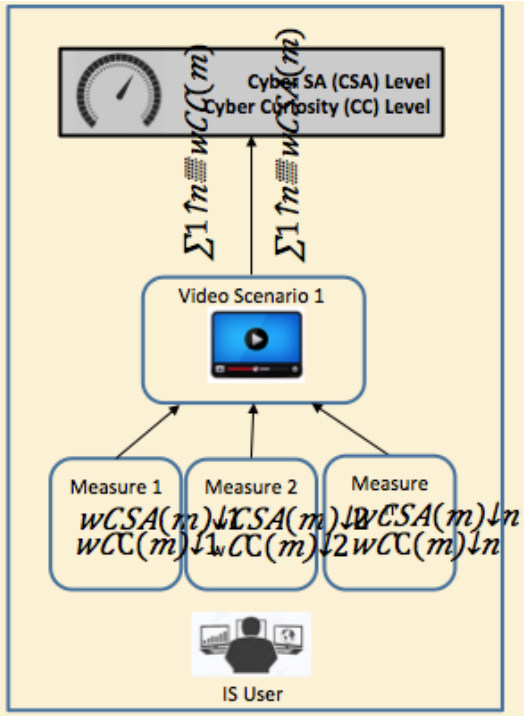


Figure 4. Conceptual design of the cyber SA and cyber curiosity measurement approach

Guillermo (Will) Perez, Ph.D. - Royal Caribbean Cruises

Dissertation title (2019): "*Cyber Situational Awareness and Cyber Curiosity Taxonomy for Understanding Susceptibility of Social Engineering Attacks in the Maritime Industry*"

Cognitive Load and Password Strength

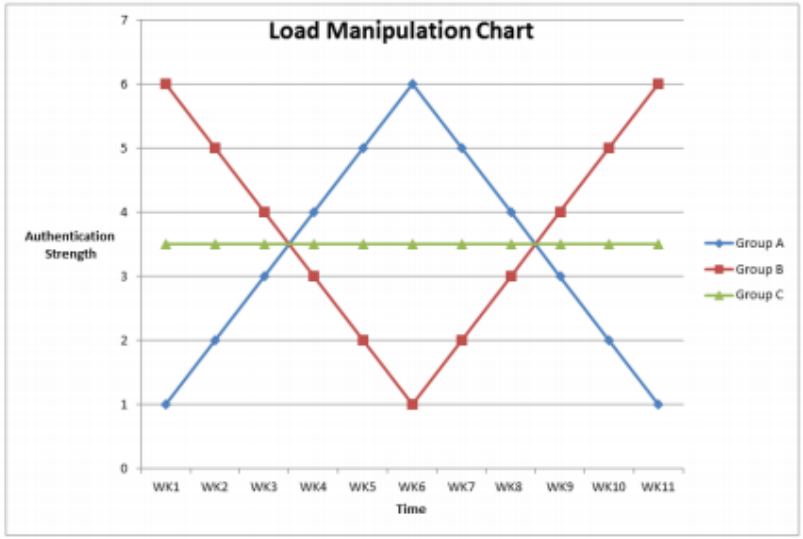


Figure 1: Load Manipulation Chart of the Authentication Strength for the Three Groups

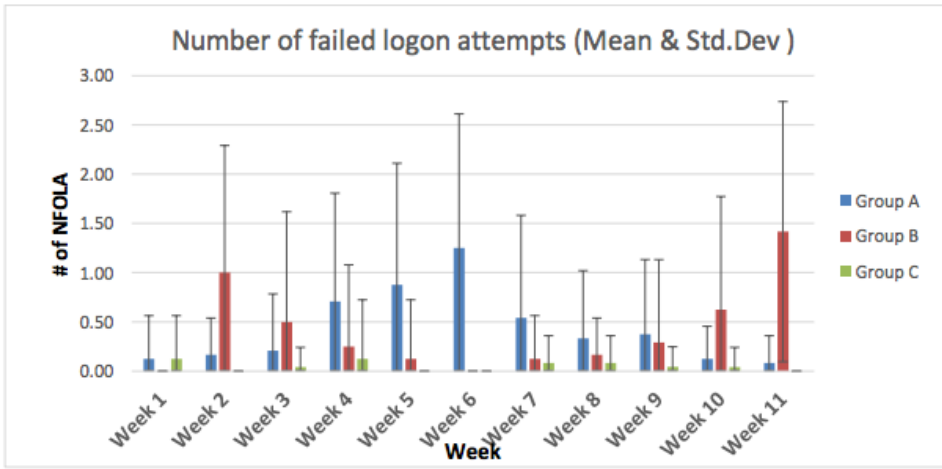


Figure 3a. Number of Failed Logon Attempts (NFOLA) Mean and SD

At what point does the increase of the cognitive load (via different password strengths) become counterproductive to the organization by causing an **increase in number of failed OS logon attempts, users' average logon times, average task completion times, and number of requests for assistance (unlock & reset account)**?

when the authentication strength is stronger than 10 characters, one uppercase, one number, and one special character it becomes counterproductive.

Stephen Mujeye, Ph.D.
Dissertation title (2016): "*An Experimental Study on the Role of Password Strength and Cognitive Load on Employee Productivity*"

Judgment Errors: Environment & Device Type

Social Engineering Attack Type

Phishing

Device	Environment: Distracting	Environment: Non-Distracting
Mobile Phone	Distracted via Mobile Phone	Not Distracted via Mobile Phone
Computer	Distracted via Computer	Not Distracted via Computer

PMSER

Device	Environment: Distracting	Environment: Non-Distracting
Mobile Phone	Distracted via Mobile Phone	Not Distracted via Mobile Phone
Computer	Distracted via Computer	Not Distracted via Computer

Figure 1. Proposed 2x2x2 Experimental Design Taxonomy of Device (Mobile Phone/Computer) vs. Environment (Distracting/Non-Distracting) vs. Social Engineering Attack Type (Phishing/PMSER)

Tommy Pollock, Ph.D. Student
Dissertation title: "*Experimental Study to Assess the Role of Environment and Device Type on the Success of Social Engineering Attacks: The Case of Judgment Errors*"
tp809 AT mynsu.nova.edu

Types of Human Error in Large Data Breaches

Price Waterhouse Coopers database

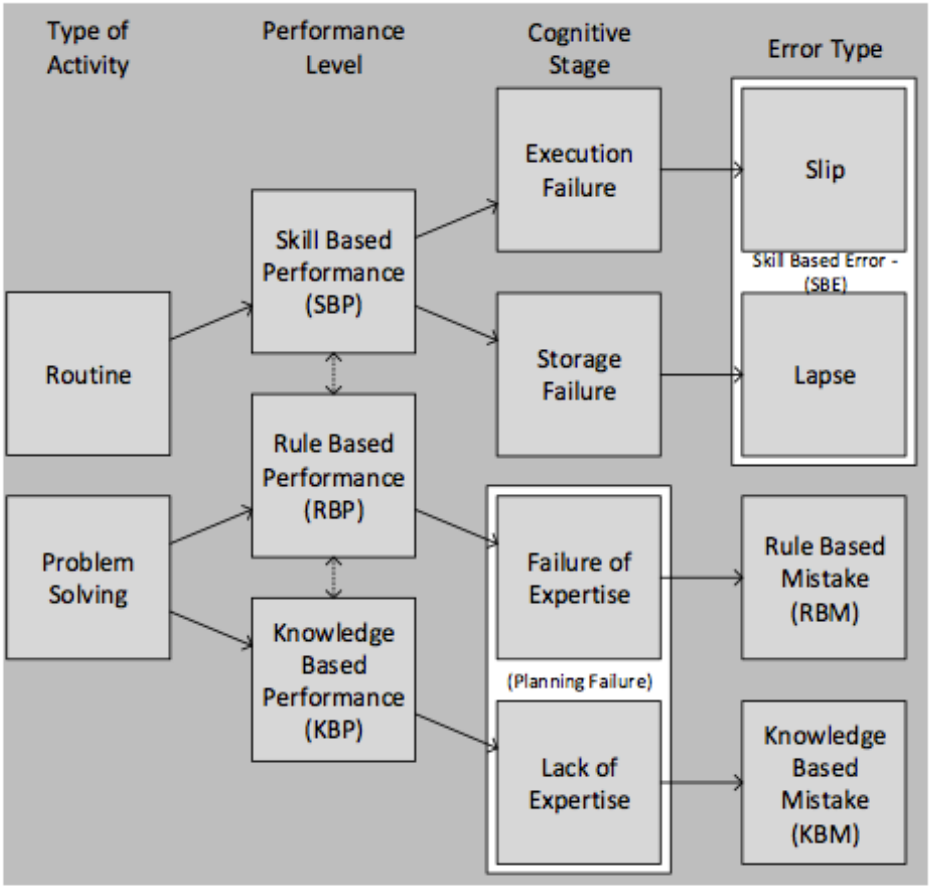
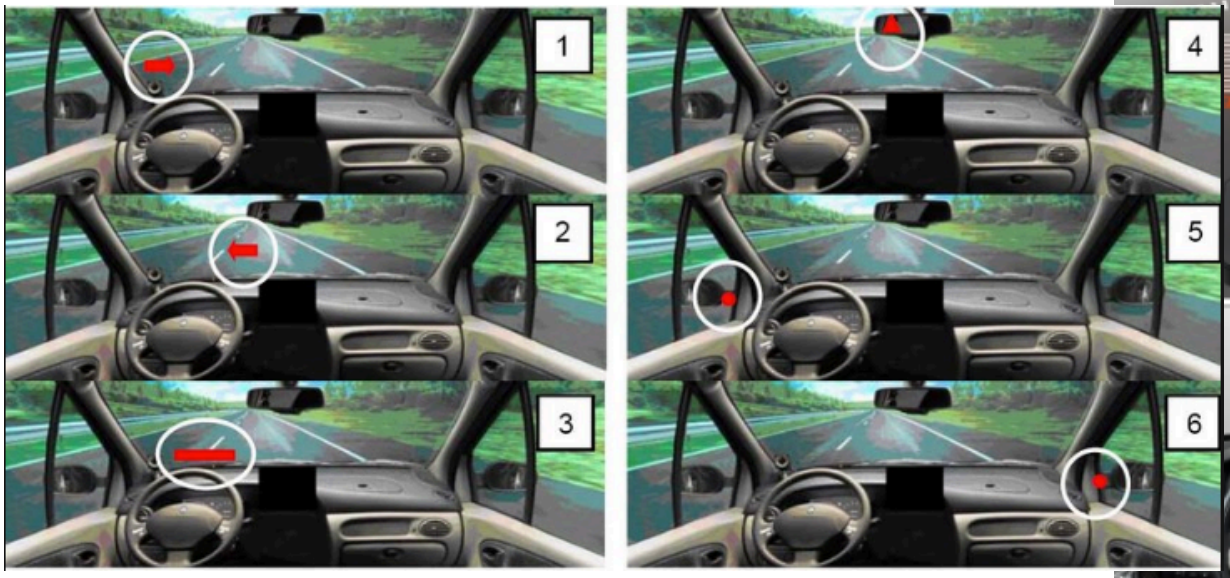


Figure 1: Generic Error-Modeling System (GEMS) adapted from Reason (1990)

Gabriel Cornejo, Ph.D. Student
Dissertation title: "*Human Errors in Cybersecurity Breaches: An Empirical Investigation using fuzzy-set Qualitative Comparative Analysis (fsQCA)*"
gc721 AT mynsu.nova.edu

Audio, Visual, and Haptics Alerts and Warnings



Molly Cooper, Ph.D. Student
Dissertation title: "*Assessment of Audio and Visual Warnings to Mitigate Risk of Phishing Attacks*"
mc3300 AT mynsu.nova.edu

Overview of the Research

- Phishing and social engineering attacks target more than 37.3 million Americans per year, and costs American organizations an average of $3.7 million annually (Abass, 2018)

- Phishing and social engineering encompass approximately 93% of information security incidents (Anti-Phishing Working Group, 2018)

- Phishing emails continue to present a significant threat to both personal and corporate data loss (Almomani, Gupta, Atawneh, Meulenberg, & Almomani, 2013; Carlton, Levy, & Ramim, 2018)

"Towards an assessment of audio and visual alerts and warnings to mitigate risk of phishing emails susceptibility" by Cooper et al. (2019)

Research Problem

- The overarching research problem this study will address is the significant volume of end users who continue to click on phishing links in emails, exposing them and/or their organizations to identity theft, monetary loss, and data loss (Aaron, 2010; Verizon, 2018)

Background

- Understanding a more aware state of mind, termed as ‘System 2 Thinking Mode’ (S2) by Kahneman (2011), describes an individual in a more aware and alert state that s/he can utilize when making important decisions (Kahneman, 2011)

Background (Cont.)

- Warnings and alerts such as: loud beeps, blinking lights or icons, and seat or steering wheel vibrations (Zheng, Tang, Qing Li, & Fei-Yue Wang, 2004) have been used to obtain a driver's attention in order to alert the driver to a potentially dangerous situation

- Meaningful warning systems reflect specific urgency and prompt the user to pay attention based on the perception of the severity of the sound, visual prompt, and other system by the end user (Sousa et al., 2016)

Study Design

- This study is a first in a sequence of several studies that will lead to the development of an audio, visual, and haptic alert and warning system to mitigate risk of phishing emails susceptibility

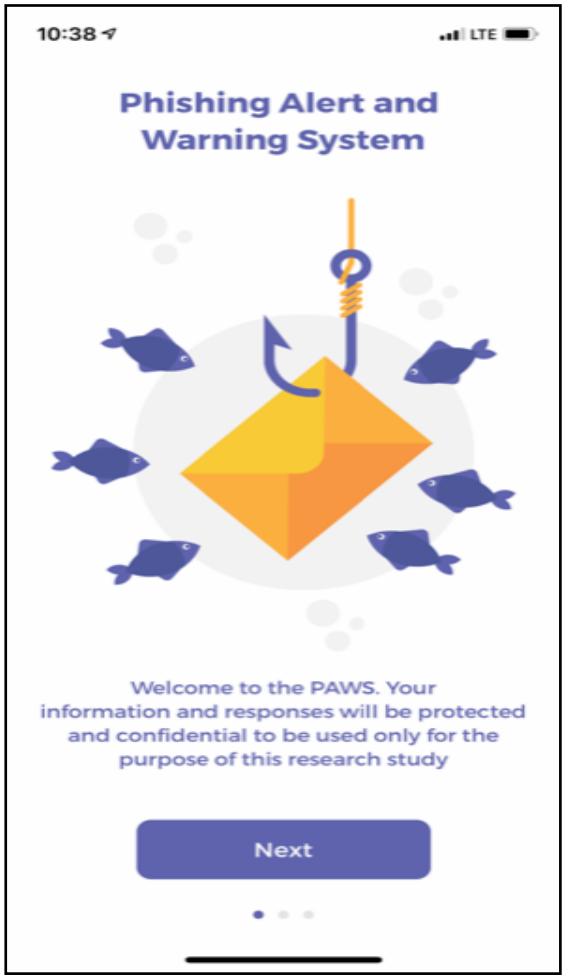
- The study will start by using Subject Matter Experts (SMEs) to ensure validity of the proposed system components

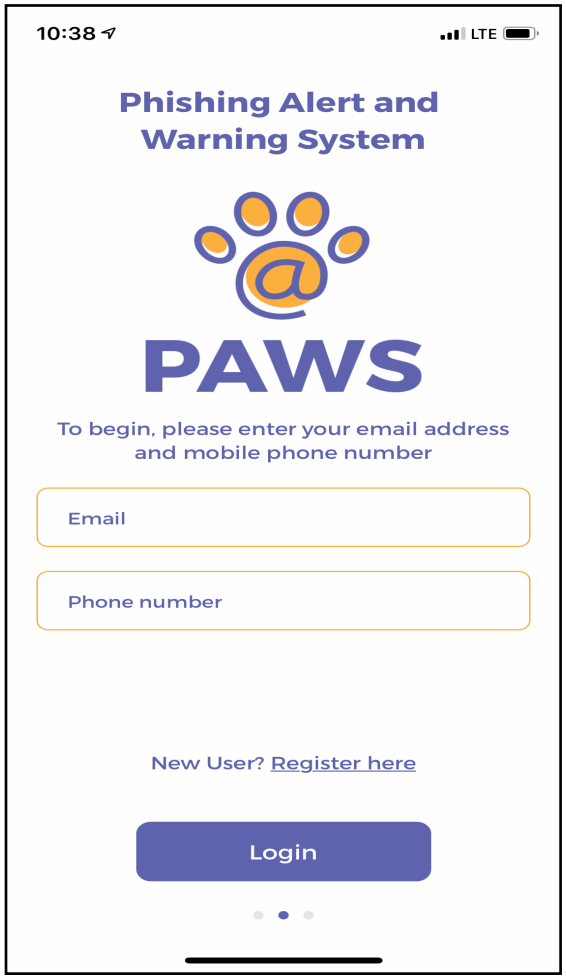
Methodology

- This research study will utilize initial qualitative and quantitative data collection phrase using approximately 25 SMEs as an expert panel (Straub, 1989).

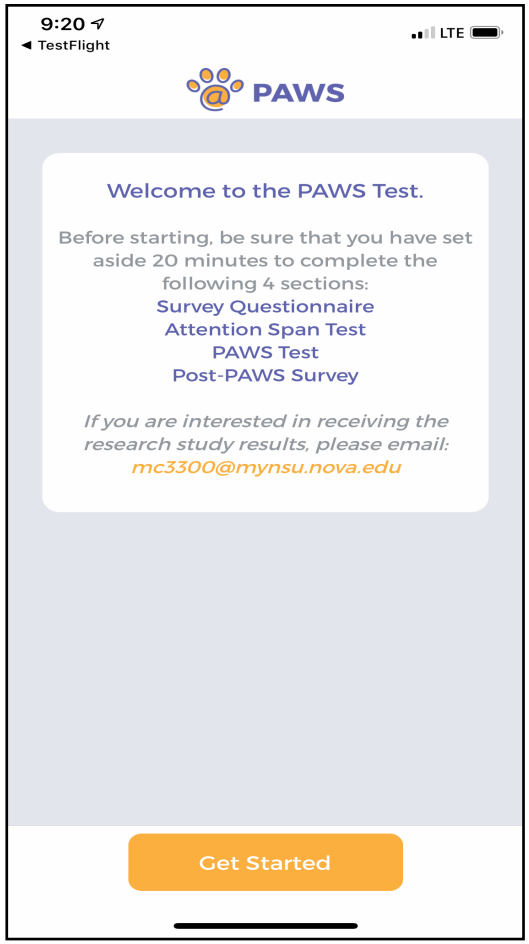
- The initial survey instrument will be conducted using Survey Monkey, using Delphi methodology for expert feedback on this subject (Ramim & Lichvar, 2014), each SME will receive an email invitation to participate in the initial survey.

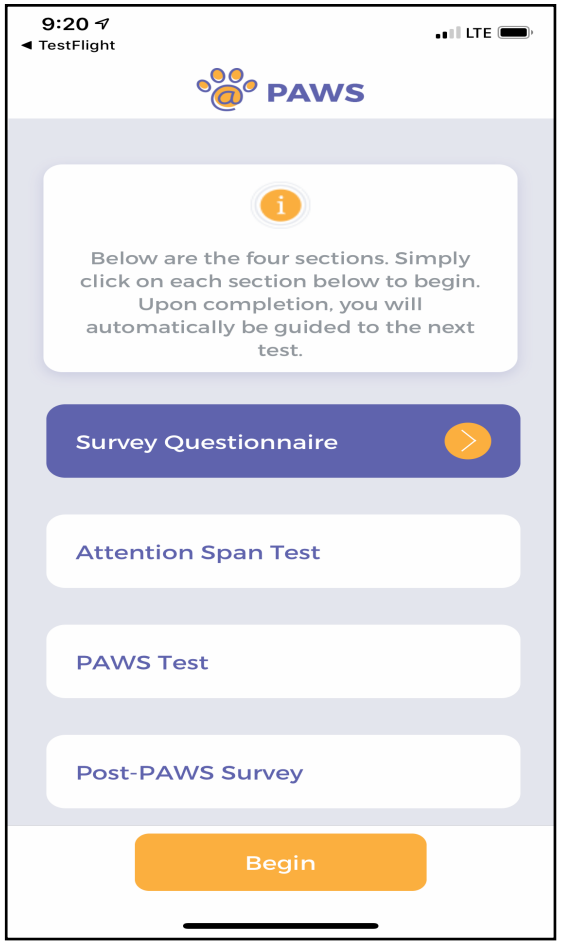
PAWS Prototype Screenshot Examples



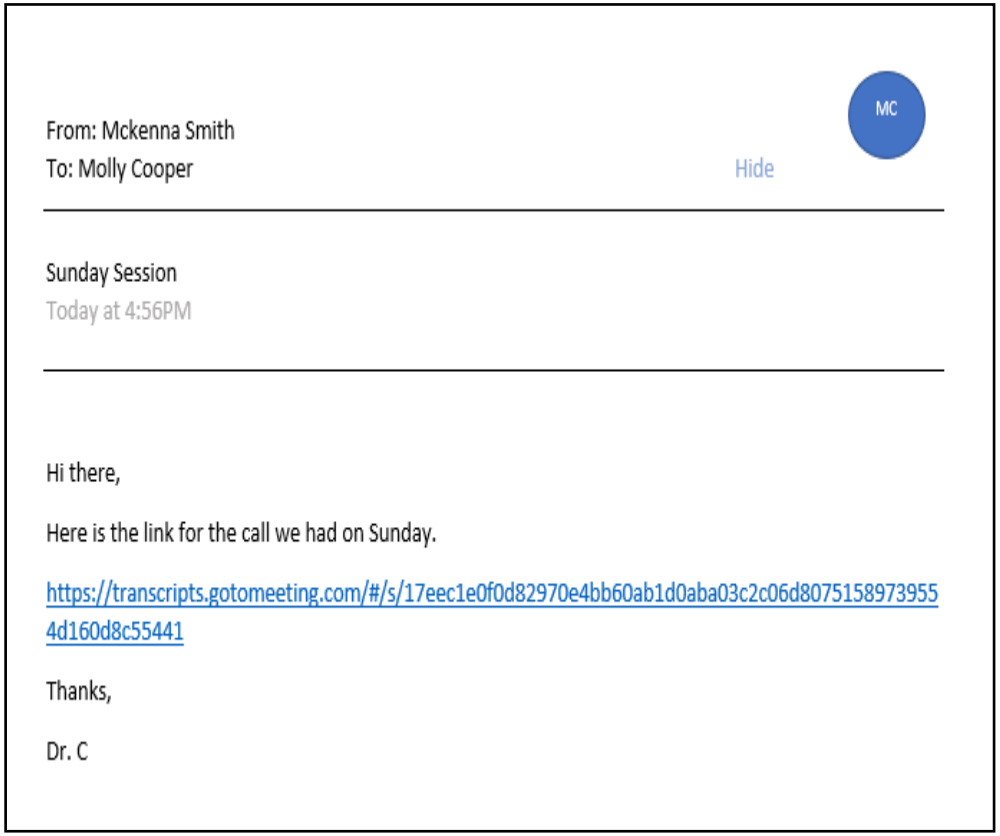


PAWS Prototype Screenshot Examples (Cont.)

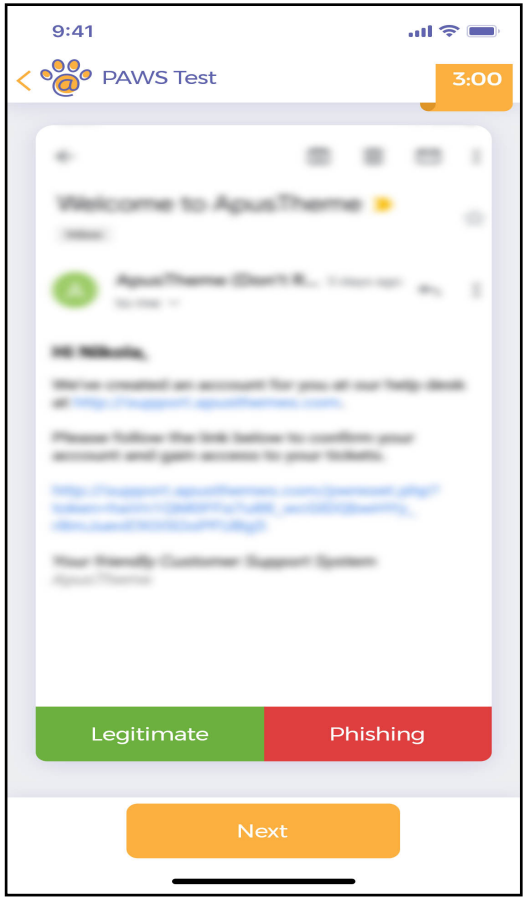


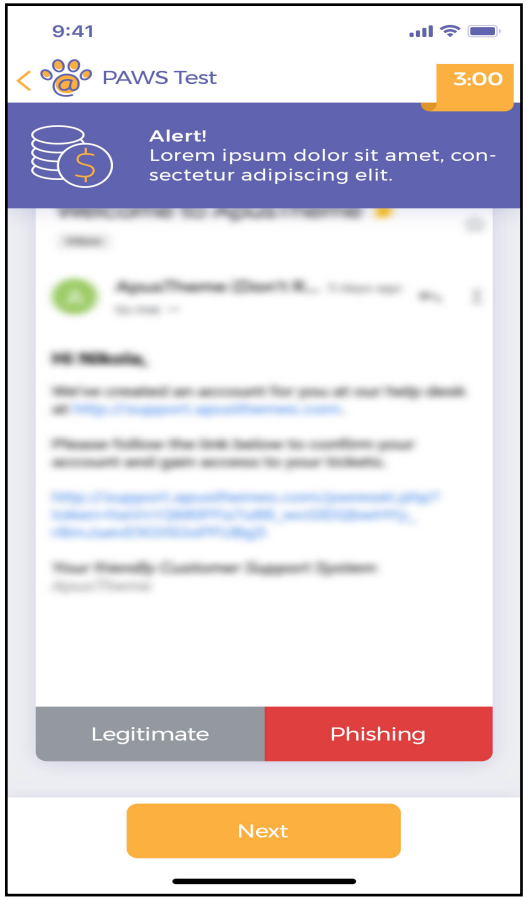


PAWS Prototype Screenshot Examples

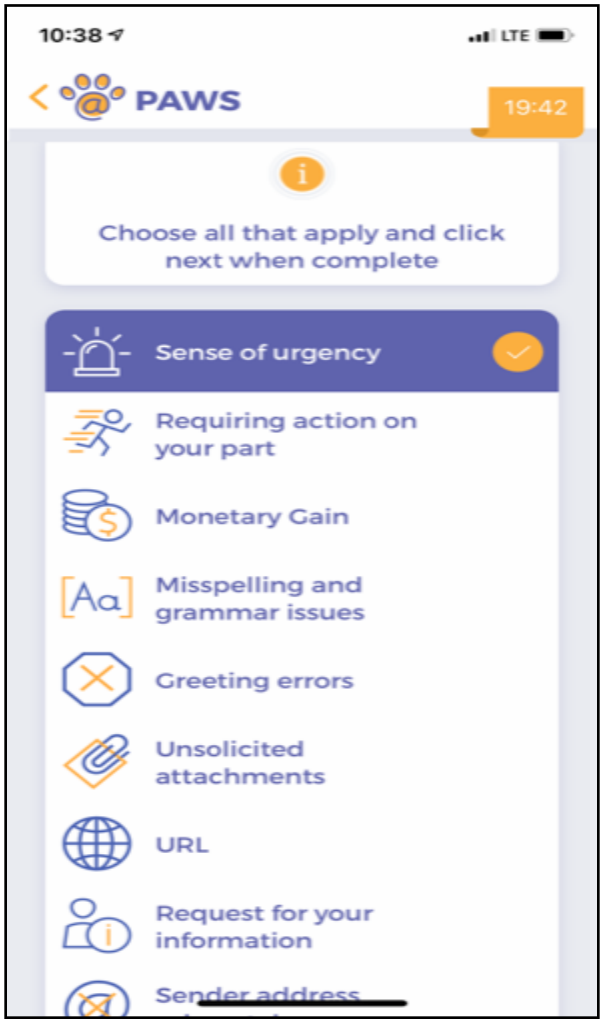


PAWS Prototype Screenshot Examples





PAWS Prototype Screenshot Examples



PAWS SME Survey

The Top 10 Signs

- SMEs will be asked to rank their Top 10 signs of phishing in emails from the survey list, and then pair each sign of phishing with what they feel would be an appropriate corresponding audio and visual alert

PAWS SME Survey (Cont.)

Signs of Phishing in Emails (15)	
Sense of urgency	Emails containing links
Requiring action from the recipient	Request for information
Monetary gain for the recipient	Spoofed content
Misspelling of words, grammar errors	Spoofed sender
Greeting errors	Unsolicited attachments
Signature errors	Threatening language
Incorrect URL	Addressing errors
Highly personalized emails	

PAWS SME Survey (Cont.)

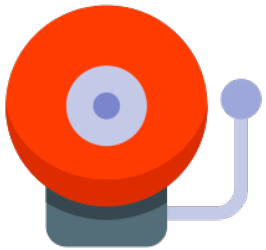
Pairings of Audio, Visual, and Haptic Alerts and Warnings:

- The survey will also contain a collection of audio, visual, and haptic alerts and warnings.
  - Audio alerts will include alarms, dings, vocal announcements, and tones
  - Visual alerts include variations of automotive dashboard icons, colors, and illustrations
  - Haptic alerts will shake at different time intervals

PAWS SME Survey (Visual Icons)

Which icon best describes the sign of phishing: Sense of Urgency?

A



B

C

PAWS SME Survey (Visual Icons, Cont.)

Which icon best describes the sign of phishing: Requiring Action from the Email Recipient?

A

B

C

Audio alerts will be presented to the participant on their mobile device. Which audio alert method is the most effective?


A.
Stock mobile device notification sounds.


B.
Household alert sounds.


C.
Automobile alert sounds.


D.
Voice over sound of each sign of phishing.

PAWS SME Survey (Cont.)

Ability and Time To Notice

- SMEs will also be asked what they feel an appropriate (a) *ability to notice* signs of phishing in emails (measured in tasks and seconds), and (b) *time to notice* signs of phishing in emails (measured tasks and seconds) would be, along with any further qualitative feedback they have on the proposed study along with proposed project

PAWS SME Survey (Cont.)

- Data collected in the SMEs survey will be used to construct an application to test (a) *ability to notice* and (b) *time to notice* phishing in emails using audio and visual warnings and alerts

- Future research will also include a qualitative and quantitative data collection with participants through an application delivery system (Straub, 1989)

PAWS SME Survey (Cont.)

How long should it take for a recipient of a phishing email to notice signs of phishing in the email?

A. Under three seconds
B. 3-5 seconds
C. 6-10 seconds
D. 11-15 seconds
E. 16-20 seconds
F. 21-25 seconds
G. 26-30 seconds
H. Over 30 seconds
I. Over 60 seconds

PAWS SME Survey (Cont.)

What is the maximum amount of time to lapse before it is determined the recipient did not notice signs of phishing in email?

A. 30 seconds
B. 40 seconds
C. 60 seconds
D. 90 seconds
E. 120 seconds

PAWS SME Survey (Cont.)

What are some of the tasks the determine a recipient's ability to detect signs of phishing in emails?

A. Clicking "Phishing" (at the bottom of the app screen)
B. Not clicking anything on the screen
C. Clicking on the signs of phishing the participant noticed (on the signs of phishing app screen)
D. Other (let's discuss!)

PAWS SME Survey (Cont.)

What determines a recipient's ability to notice signs of phishing in emails?
(Choose all that apply)

A. The time it takes to click "Phishing" or "Legitimate" email. (The PAWS app has both options to choose from)
B. The participant's age
C. The participant's gender
D. The participant's native and secondary languages spoken
E. The participant's attention span
F. The participant's experience with reading emails on a mobile device
G. The participant's experience with phishing training

Discussion and Conclusions

- Phishing attacks, a type of social engineering, is still a problem that needs to be solved or at least contribute to the body of research that aims at reducing phishing susceptibility among end users

- This research proposes to reduce phishing susceptibility among end users by developing a prototype that alerts end users to the signs of phishing in emails with audio and visual alerting

Future Work

- Future work includes constructing a prototype application that delivers the signs of phishing in emails with appropriate audio, visual, and haptic warnings and alerts as determined by SMEs feedback

- Participants will be tested on (a) *ability to notice* and (b) *time to notice* signs of phishing in emails with and without the assistance of audio and visual warning and alerting

Would you like to participate in the SME survey?

Please email Molly Cooper at:
mc3300@mynsu.nova.edu

Thank you!

Center for Information Protection, Education, and Research (CIPhER): http://infosec.nova.edu/

Levy CyLab: http://CyLab.nova.edu/