The Human Factor in Cybersecurity: The Role of Environment and Device Type on Social Engineering Attacks

Presented by
Tommy Pollock and Yair Levy

TIDEWATER COMMUNITY COLLEGE
From here, go anywhere.™

College of Computing and Engineering
NOVA SOUTHEASTERN UNIVERSITY
NSU Florida

http://CyLab.nova.edu/

Our Speakers For Today's Webinar

Yair Levy, Ph.D.
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. His research is focused on Social Engineering and cyber threat mitigation. 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 has been consulting to local, state, and federal agencies including the National Security Agency (NSA) on cybersecurity related matters. 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

Tommy Pollock
Ph.D. Candidate
Adjunct IT Instructor
Tidewater Community College

Tommy Pollock is an Adjunct IT Certification Instructor and IT Coordinator at the Tidewater Community College Center for Workforce Development. Mr. Pollock develops all of the IT course curriculum and provides cybersecurity seminars for various workshops. He also tutors cybersecurity and statistics part time for undergraduate students.

His primary research interests are human error and social engineering in cybersecurity. He holds both undergraduate degrees in IS Security and Management and is currently pursuing a Ph.D. in Information Assurance

LEVY CyLAB

The research in our laboratory focuses on the ***human factor in cybersecurity*** of all three cybersecurity landscape pillars with emphasis on addressing the following three key research areas and their interconnections: Cybersecurity threat mitigation, Social-Engineering, and user-authentication.

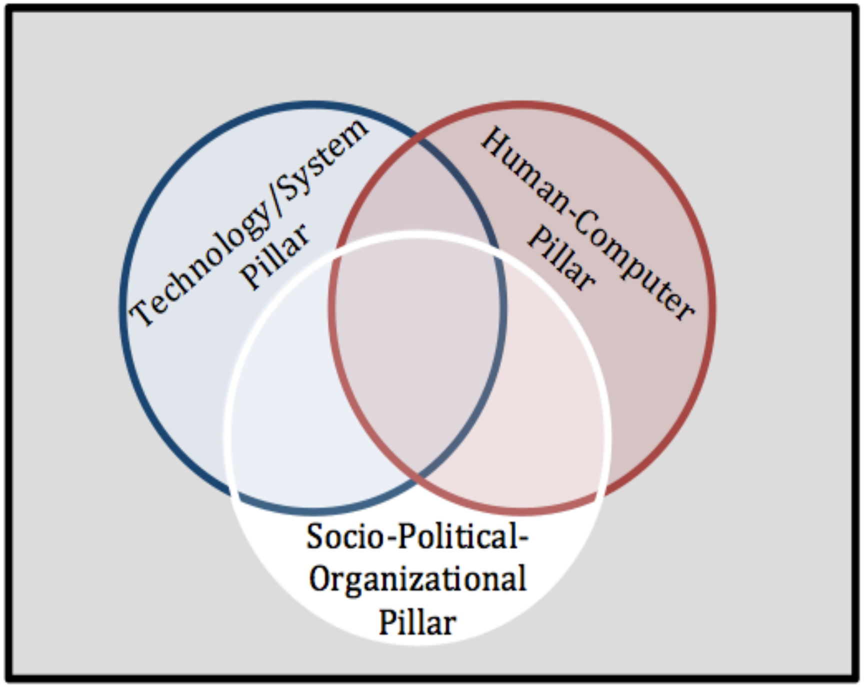
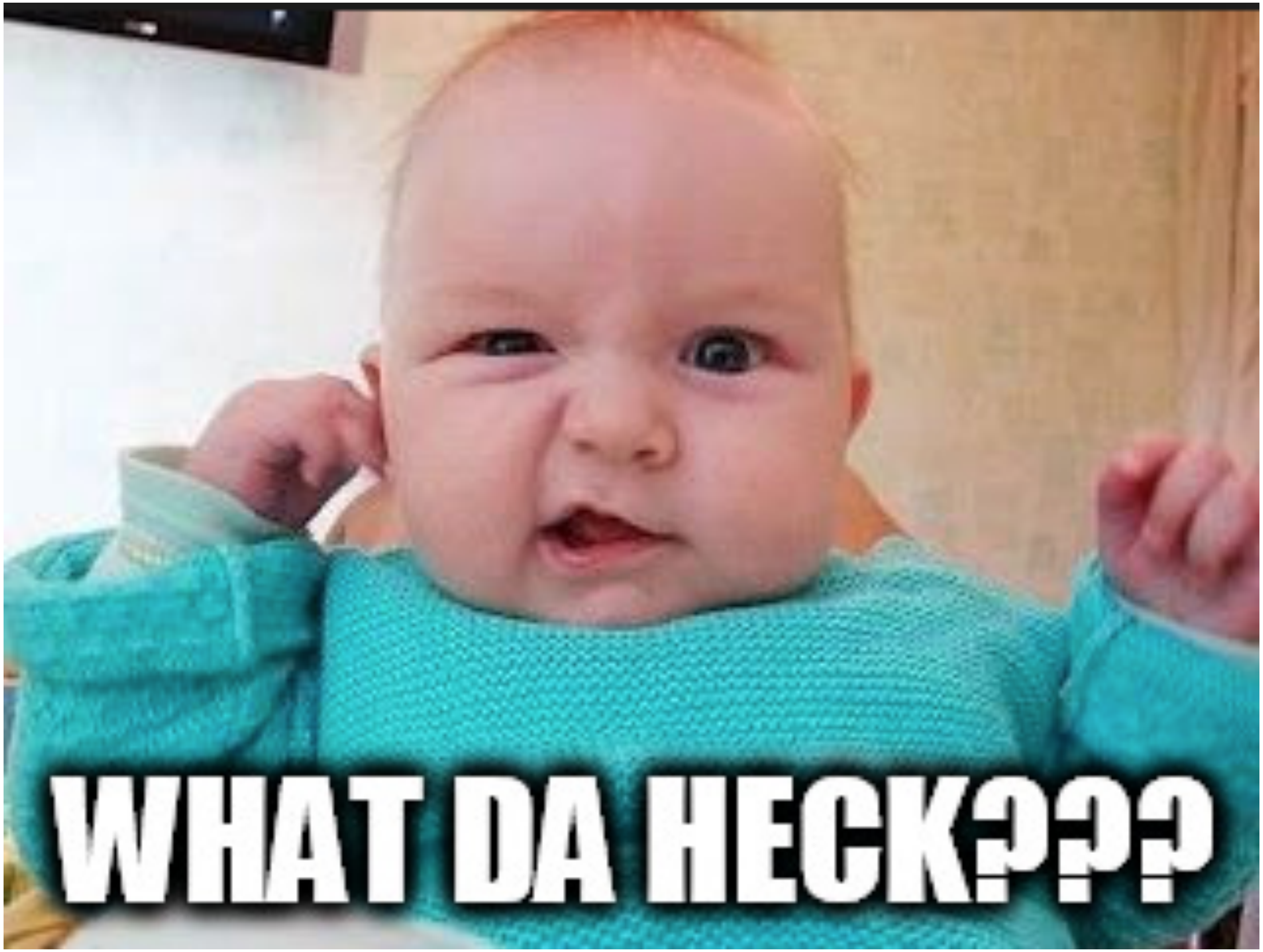


Figure 1: The Cybersecurity Landscape

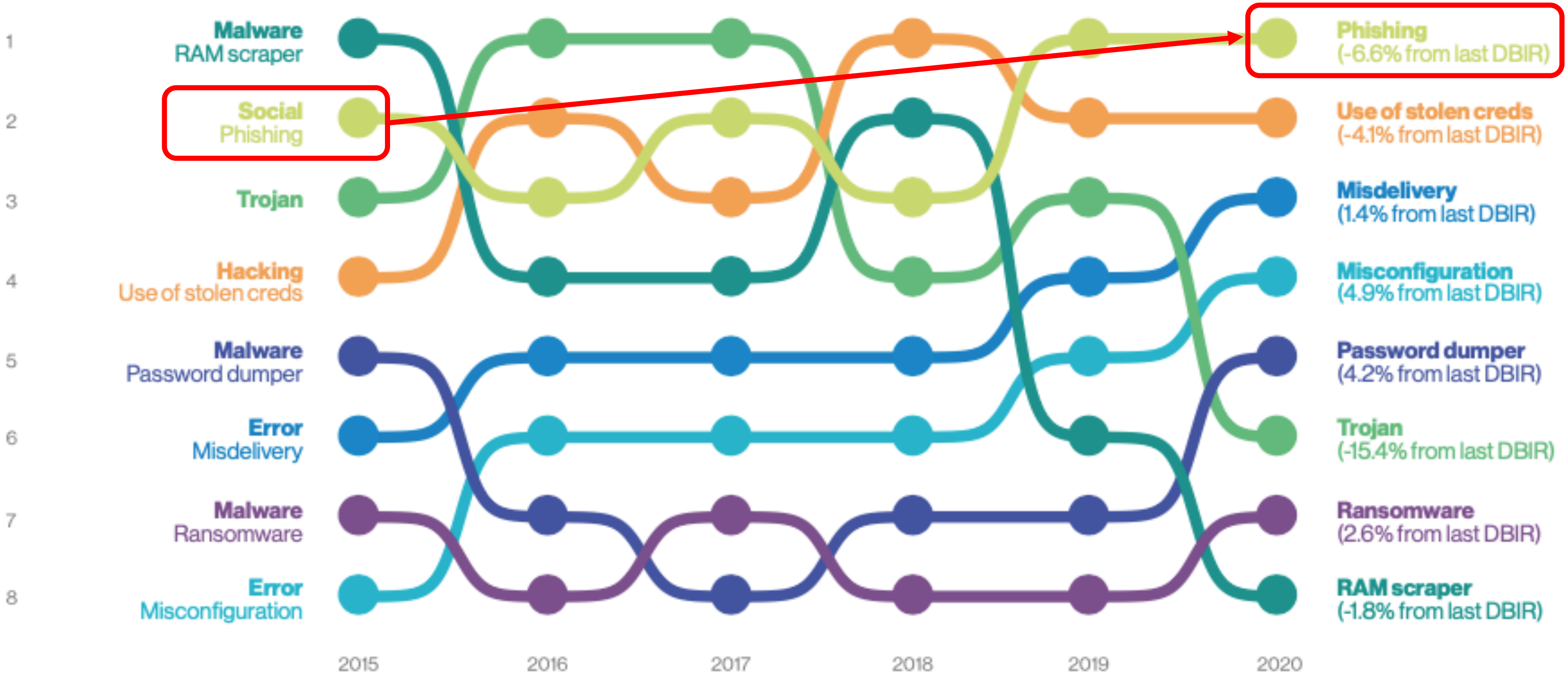
http://CyLab.nova.edu/

Human Factor in Cybersecurity?



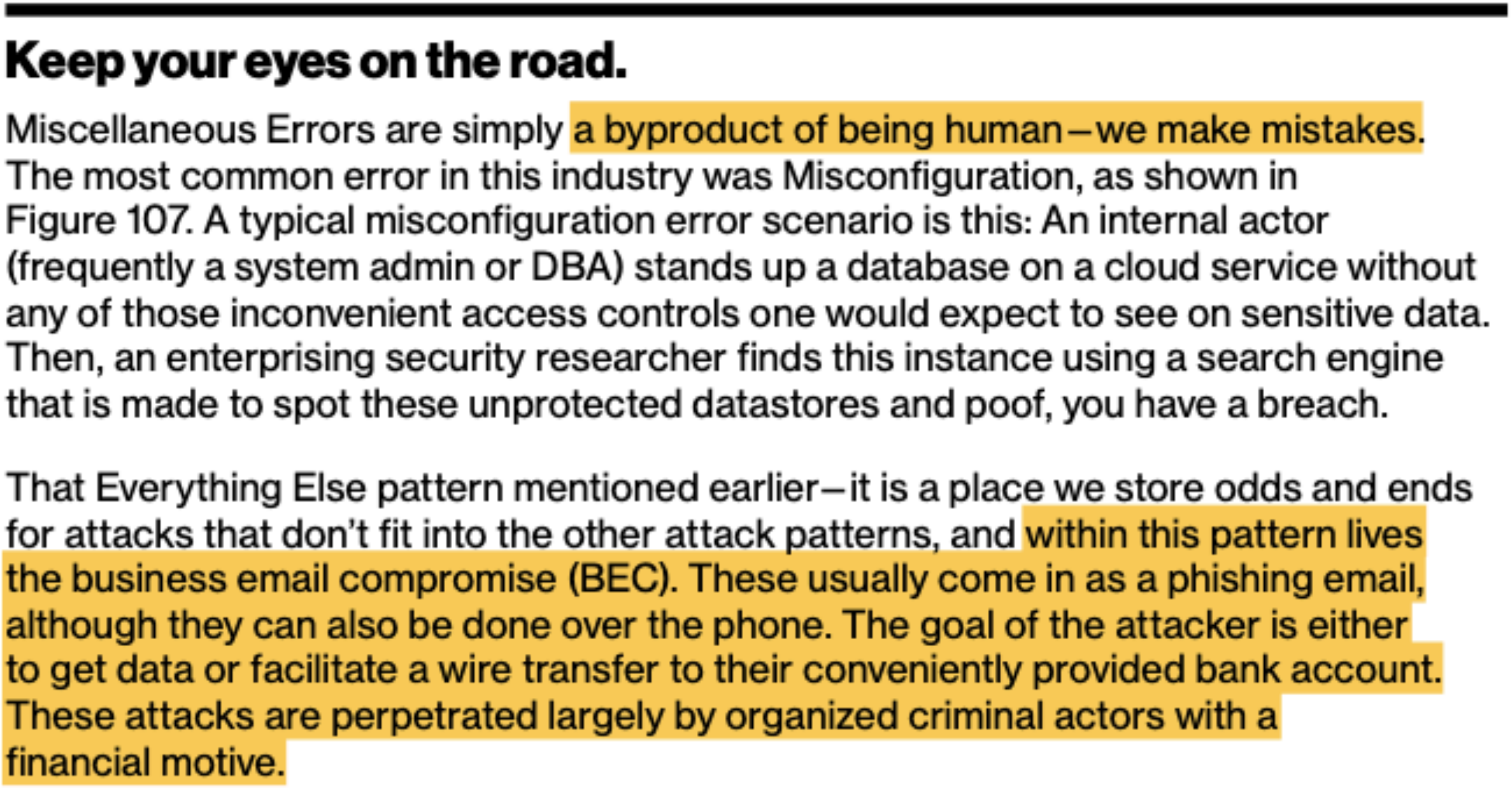
Human Factor in Cybersecurity?

Figure 6. Select action varieties in breaches over time



Source: 2020 Verizon's Data Breach Investigations Report (DBIR), p. 9

Human Factor in Cybersecurity?



Keep your eyes on the road.

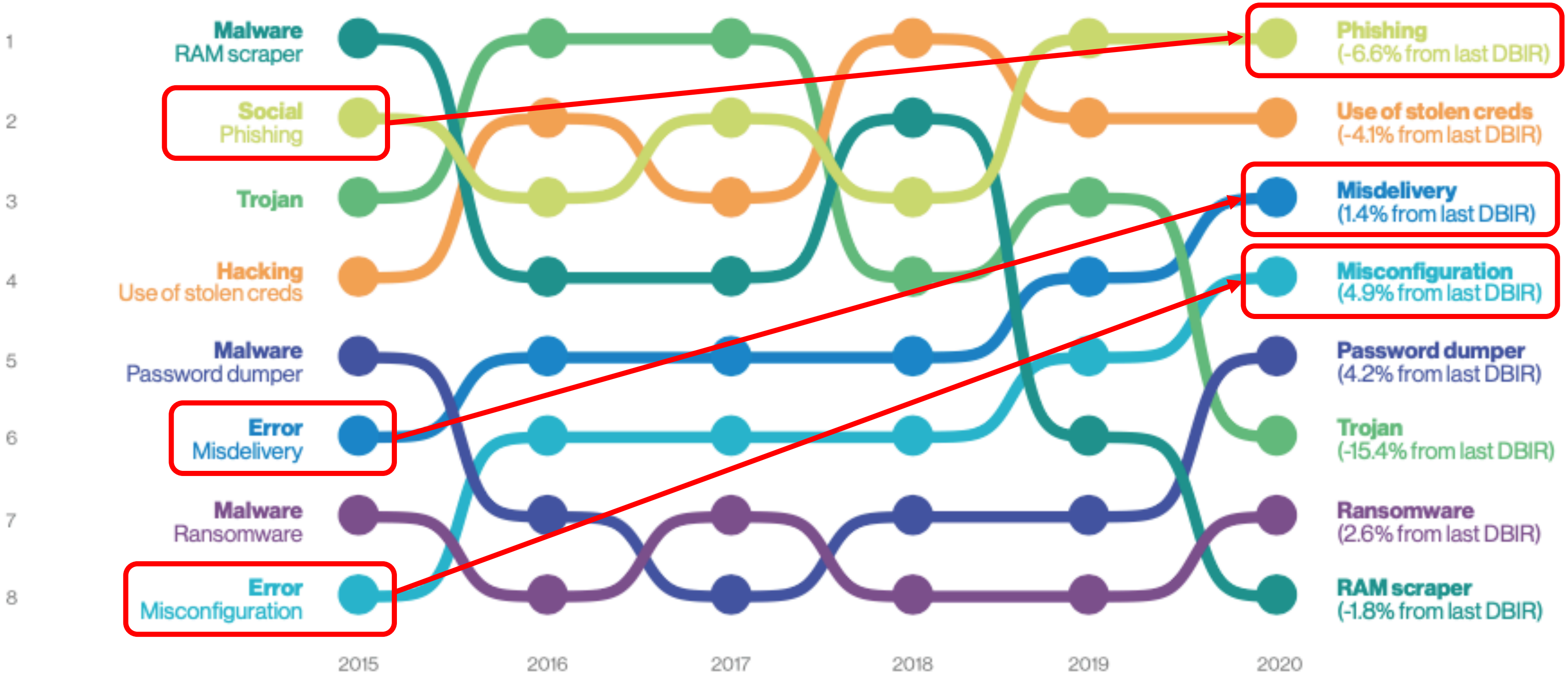
Miscellaneous Errors are simply a byproduct of being human—we make mistakes. The most common error in this industry was Misconfiguration, as shown in Figure 107. A typical misconfiguration error scenario is this: An internal actor (frequently a system admin or DBA) stands up a database on a cloud service without any of those inconvenient access controls one would expect to see on sensitive data. Then, an enterprising security researcher finds this instance using a search engine that is made to spot these unprotected datastores and poof, you have a breach.

That Everything Else pattern mentioned earlier—it is a place we store odds and ends for attacks that don't fit into the other attack patterns, and within this pattern lives the business email compromise (BEC). These usually come in as a phishing email, although they can also be done over the phone. The goal of the attacker is either to get data or facilitate a wire transfer to their conveniently provided bank account. These attacks are perpetrated largely by organized criminal actors with a financial motive.

Source: 2020 Verizon's Data Breach Investigations Report (DBIR), p. 77

Human Factor in Cybersecurity?

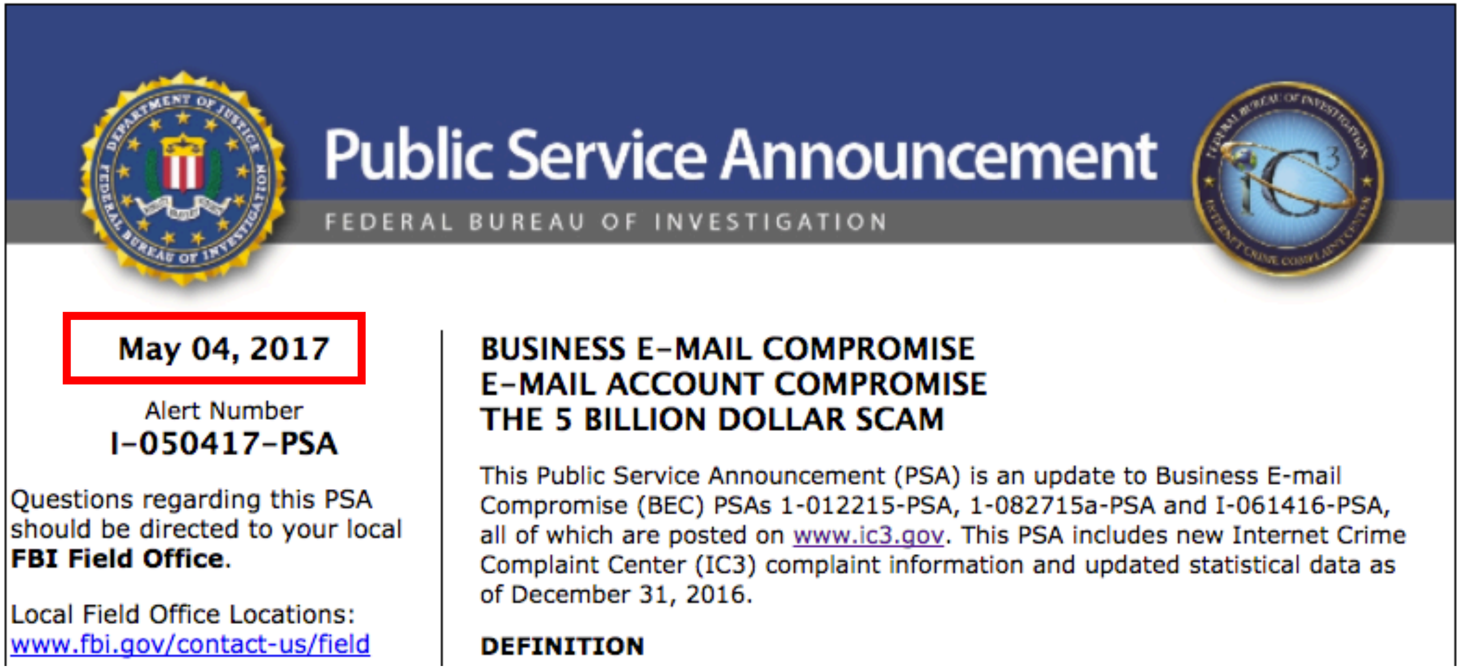
Figure 6. Select action varieties in breaches over time



Source: 2020 Verizon's Data Breach Investigations Report (DBIR), p. 9

Human Factor in Cybersecurity?

Social Engineering – Business E-mail Compromise (BEC) - 2017



Public Service Announcement

FEDERAL BUREAU OF INVESTIGATION

May 04, 2017

Alert Number

I-050417-PSA

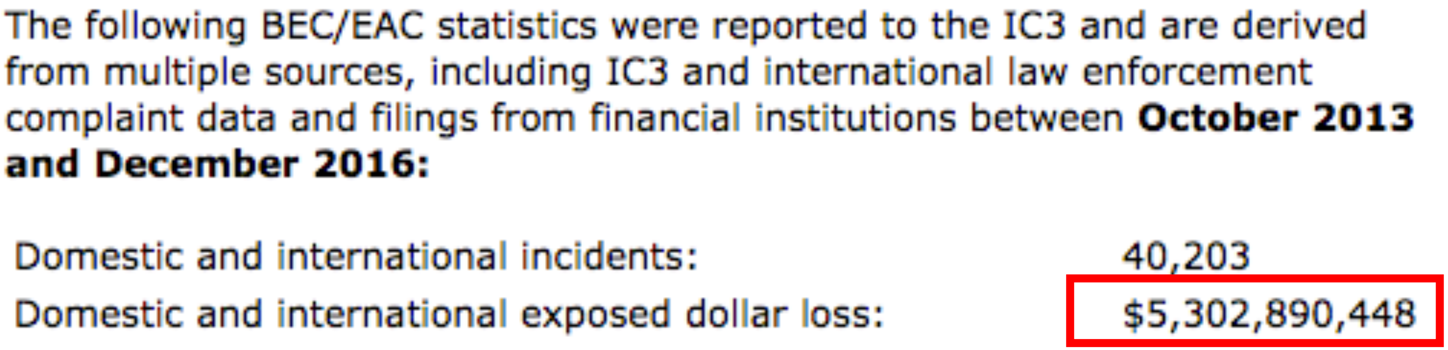
Questions regarding this PSA should be directed to your local **FBI Field Office.**

Local Field Office Locations: www.fbi.gov/contact-us/field

BUSINESS E-MAIL COMPROMISE
E-MAIL ACCOUNT COMPROMISE
THE 5 BILLION DOLLAR SCAM

This Public Service Announcement (PSA) is an update to Business E-mail Compromise (BEC) PSAs 1-012215-PSA, 1-082715a-PSA and I-061416-PSA, all of which are posted on www.ic3.gov. This PSA includes new Internet Crime Complaint Center (IC3) complaint information and updated statistical data as of December 31, 2016.

DEFINITION



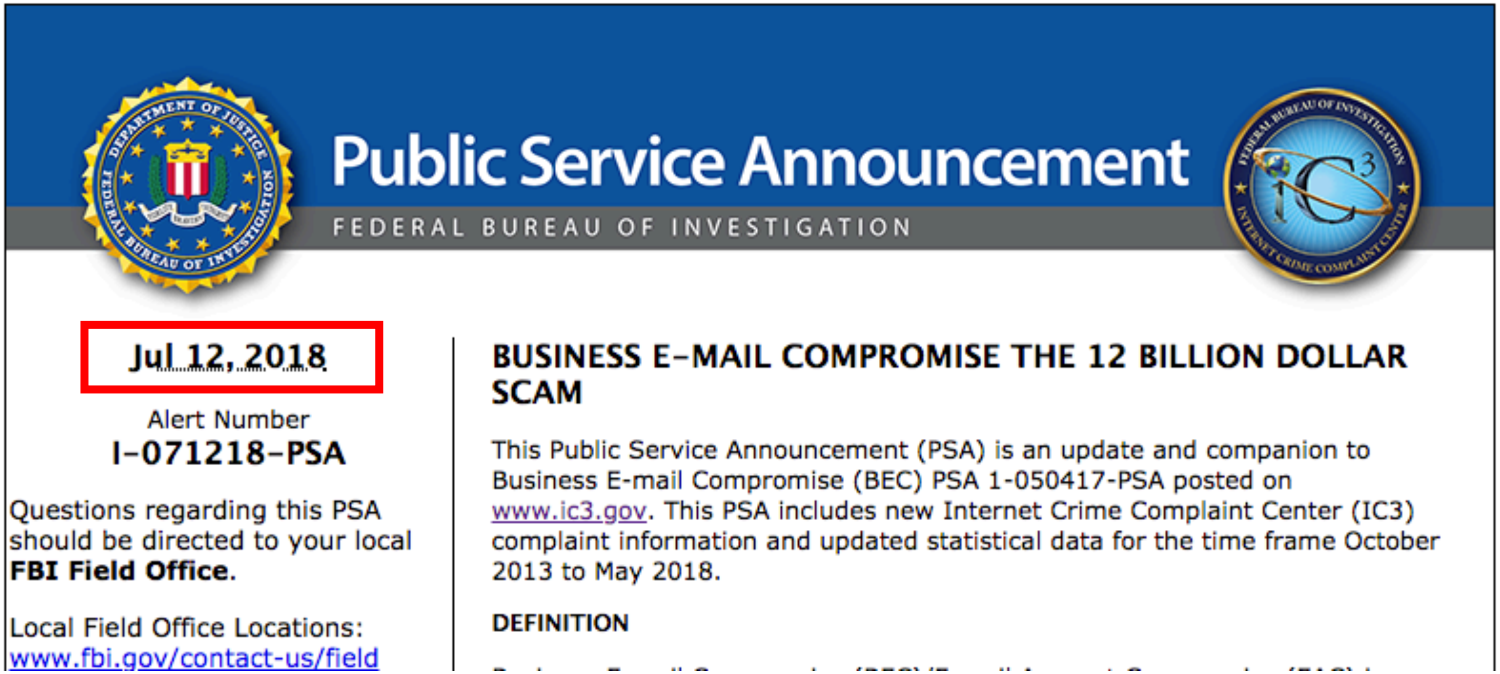
The following BEC/EAC statistics were reported to the IC3 and are derived from multiple sources, including IC3 and international law enforcement complaint data and filings from financial institutions between **October 2013 and December 2016:**

Domestic and international incidents:	40,203
Domestic and international exposed dollar loss:	$5,302,890,448

Source: FBI Internet Computer Complaint Center (IC3.gov)

Human Factor in Cybersecurity?

Social Engineering – Business E-mail Compromise (BEC) - 2018



Public Service Announcement

FEDERAL BUREAU OF INVESTIGATION

Jul 12, 2018

Alert Number

I-071218-PSA

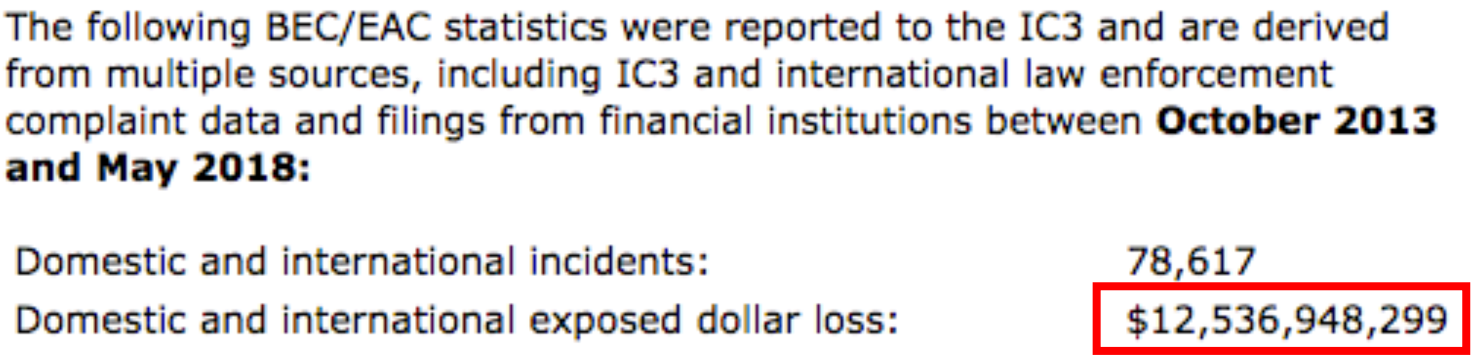
Questions regarding this PSA should be directed to your local **FBI Field Office.**

Local Field Office Locations: www.fbi.gov/contact-us/field

BUSINESS E-MAIL COMPROMISE THE 12 BILLION DOLLAR SCAM

This Public Service Announcement (PSA) is an update and companion to Business E-mail Compromise (BEC) PSA 1-050417-PSA posted on www.ic3.gov. This PSA includes new Internet Crime Complaint Center (IC3) complaint information and updated statistical data for the time frame October 2013 to May 2018.

DEFINITION



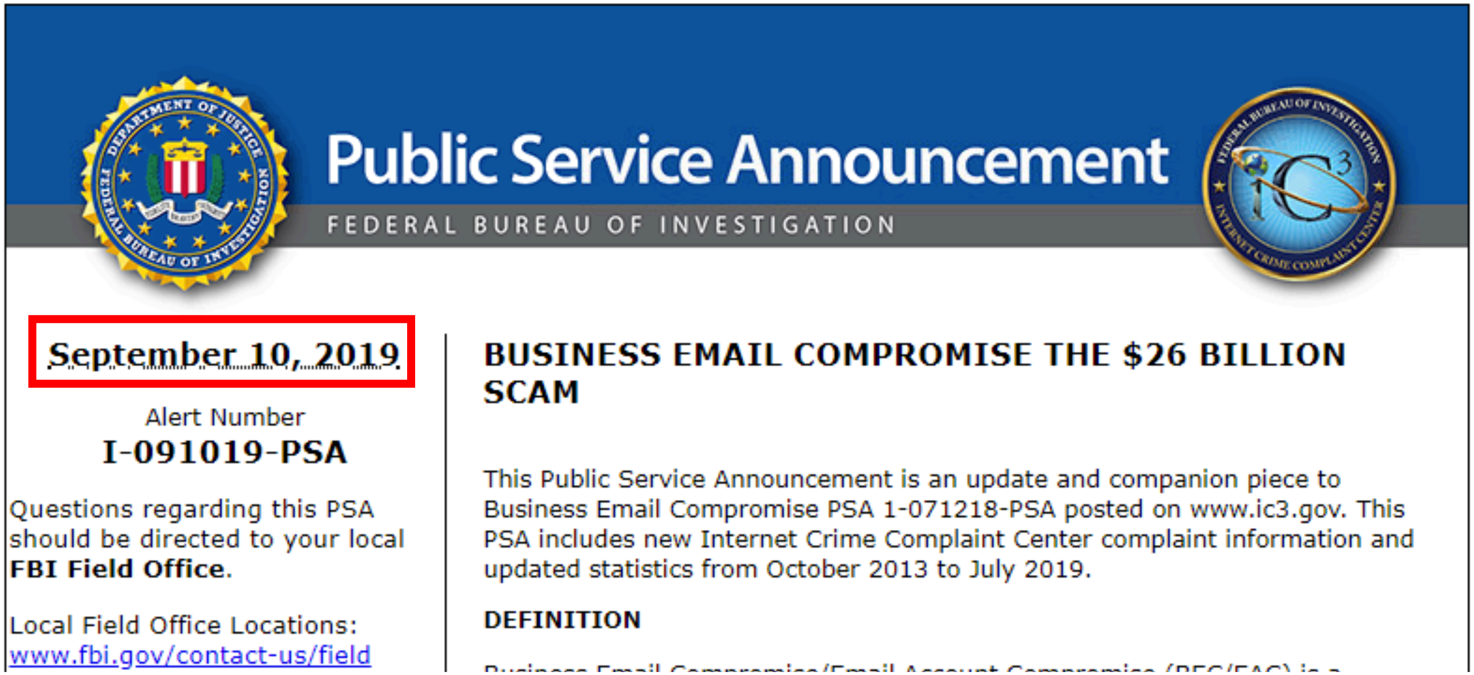
The following BEC/EAC statistics were reported to the IC3 and are derived from multiple sources, including IC3 and international law enforcement complaint data and filings from financial institutions between **October 2013 and May 2018:**

Domestic and international incidents:	78,617
Domestic and international exposed dollar loss:	$12,536,948,299

Source: FBI Internet Computer Complaint Center (IC3.gov)

Human Factor in Cybersecurity?

Social Engineering – Business E-mail Compromise (BEC) - 2019



September 10, 2019

Alert Number

I-091019-PSA

Questions regarding this PSA should be directed to your local **FBI Field Office.**

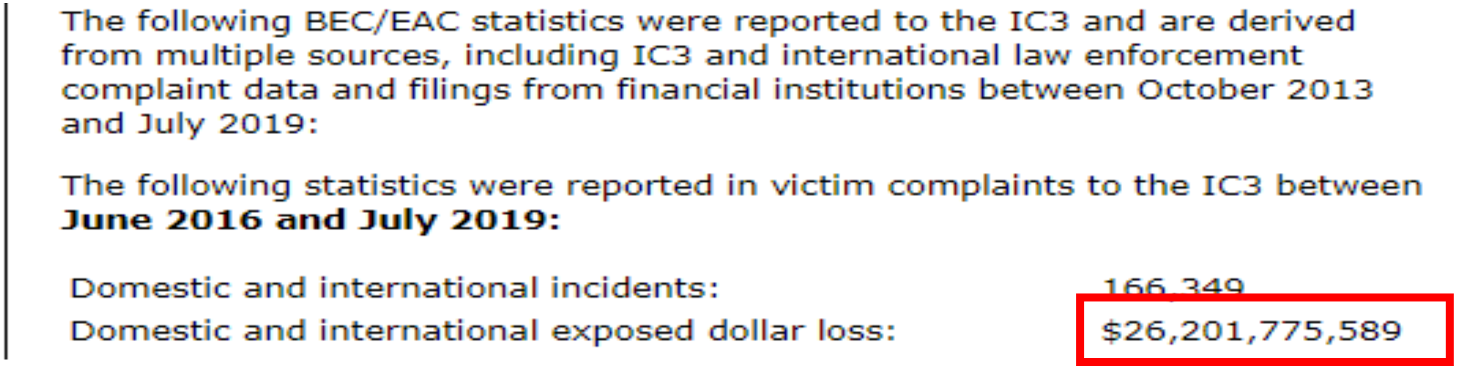
Local Field Office Locations: www.fbi.gov/contact-us/field

BUSINESS EMAIL COMPROMISE THE $26 BILLION SCAM

This Public Service Announcement is an update and companion piece to Business Email Compromise PSA 1-071218-PSA posted on www.ic3.gov. This PSA includes new Internet Crime Complaint Center complaint information and updated statistics from October 2013 to July 2019.

DEFINITION

Business Email Compromise/Email Account Compromise (BEC/EAC) is a



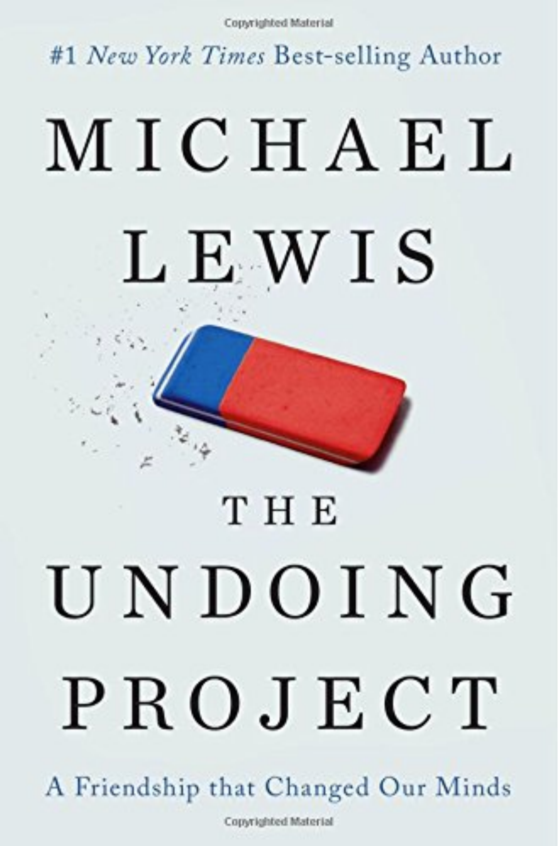
The following BEC/EAC statistics were reported to the IC3 and are derived from multiple sources, including IC3 and international law enforcement complaint data and filings from financial institutions between October 2013 and July 2019:

The following statistics were reported in victim complaints to the IC3 between **June 2016 and July 2019:**

Domestic and international incidents:	166,349
Domestic and international exposed dollar loss:	$26,201,775,589

Source: FBI Internet Computer Complaint Center (IC3.gov)

Some Theoretical Concepts:

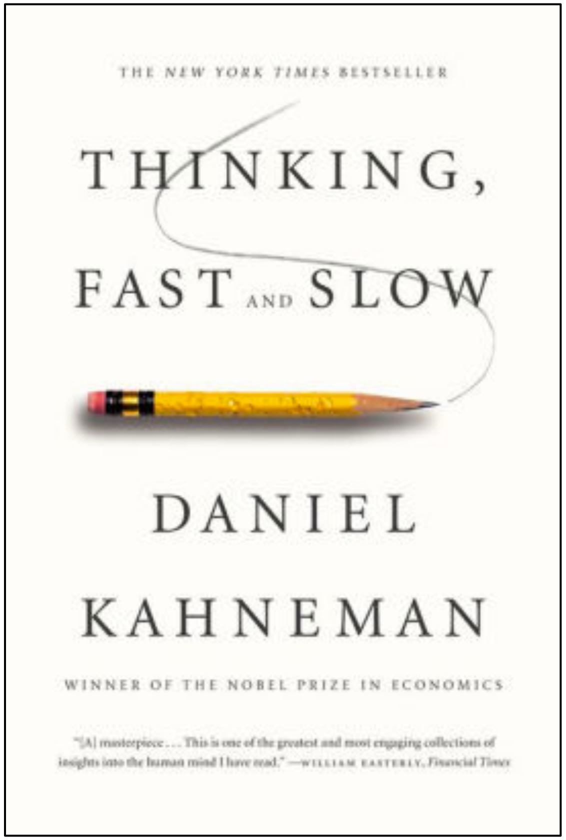


#1 *New York Times* Best-selling Author

MICHAEL LEWIS

THE UNDOING PROJECT

A Friendship that Changed Our Minds



THE *NEW YORK TIMES* BESTSELLER

THINKING, FAST AND SLOW

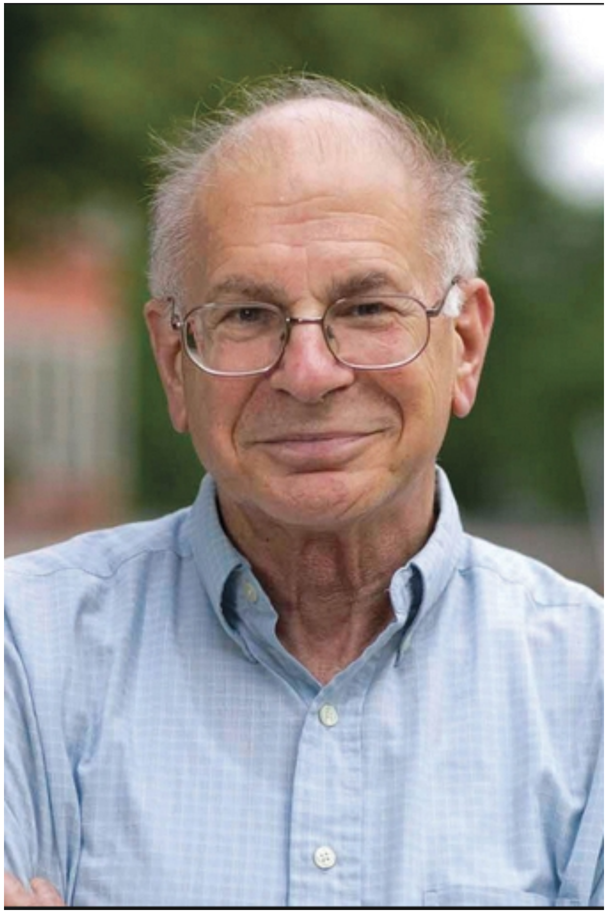
DANIEL KAHNEMAN

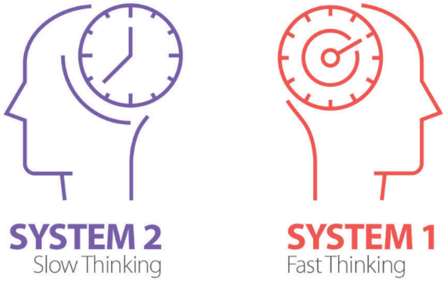
WINNER OF THE NOBEL PRIZE IN ECONOMICS

"[A] masterpiece . . . This is one of the greatest and most engaging collections of insights into the human mind I have read." —WILLIAM EASTERLY, *Financial Times*

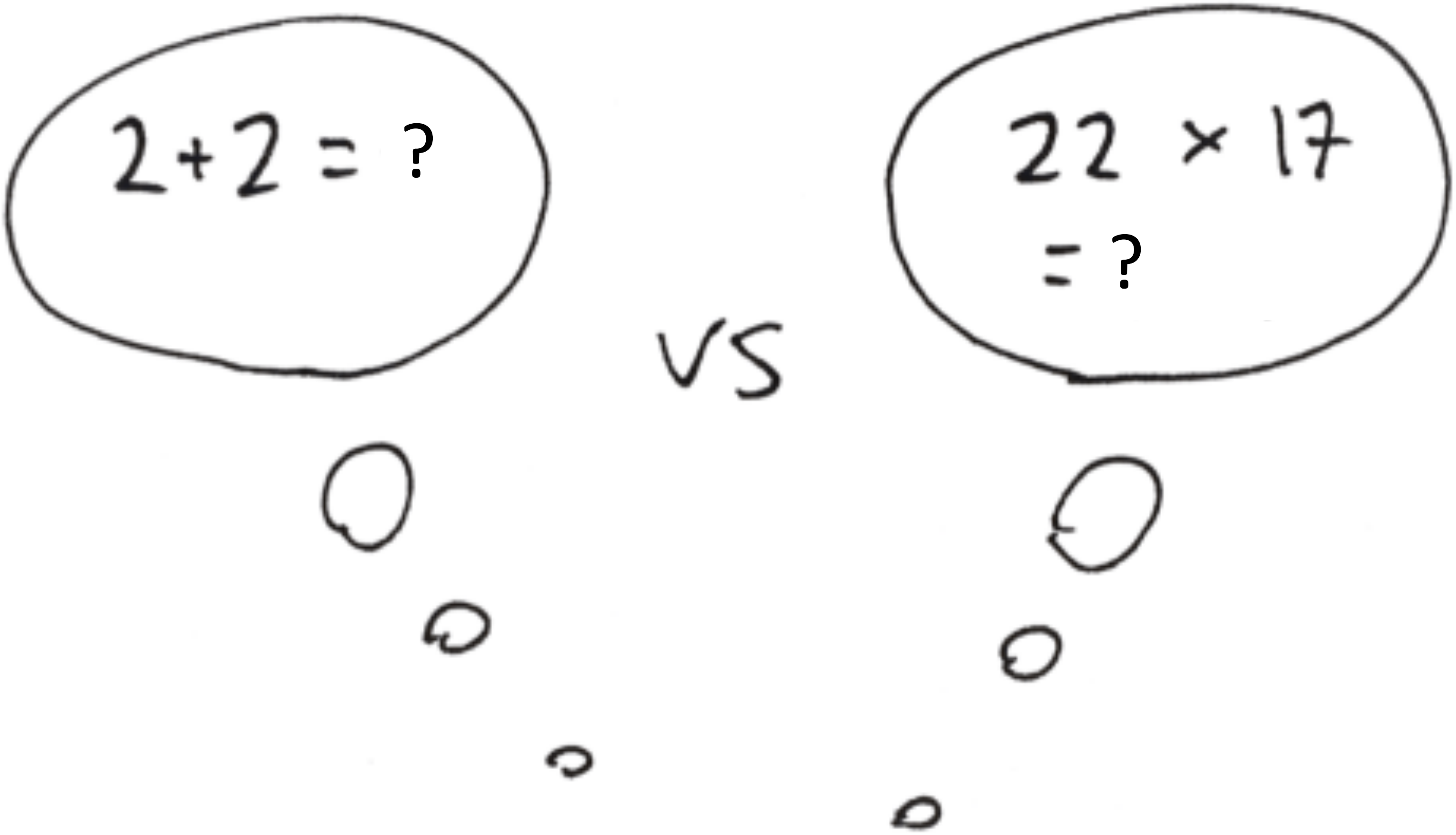
Dr. Daniel Kahneman

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.

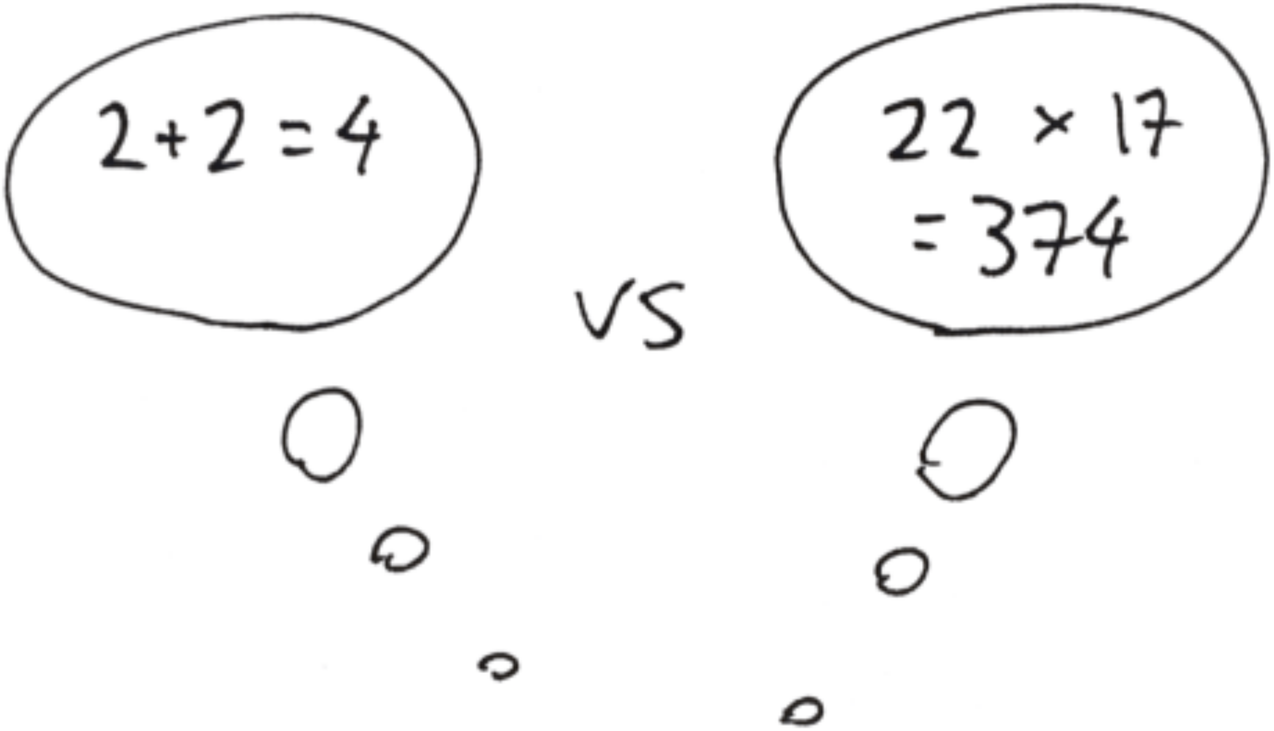


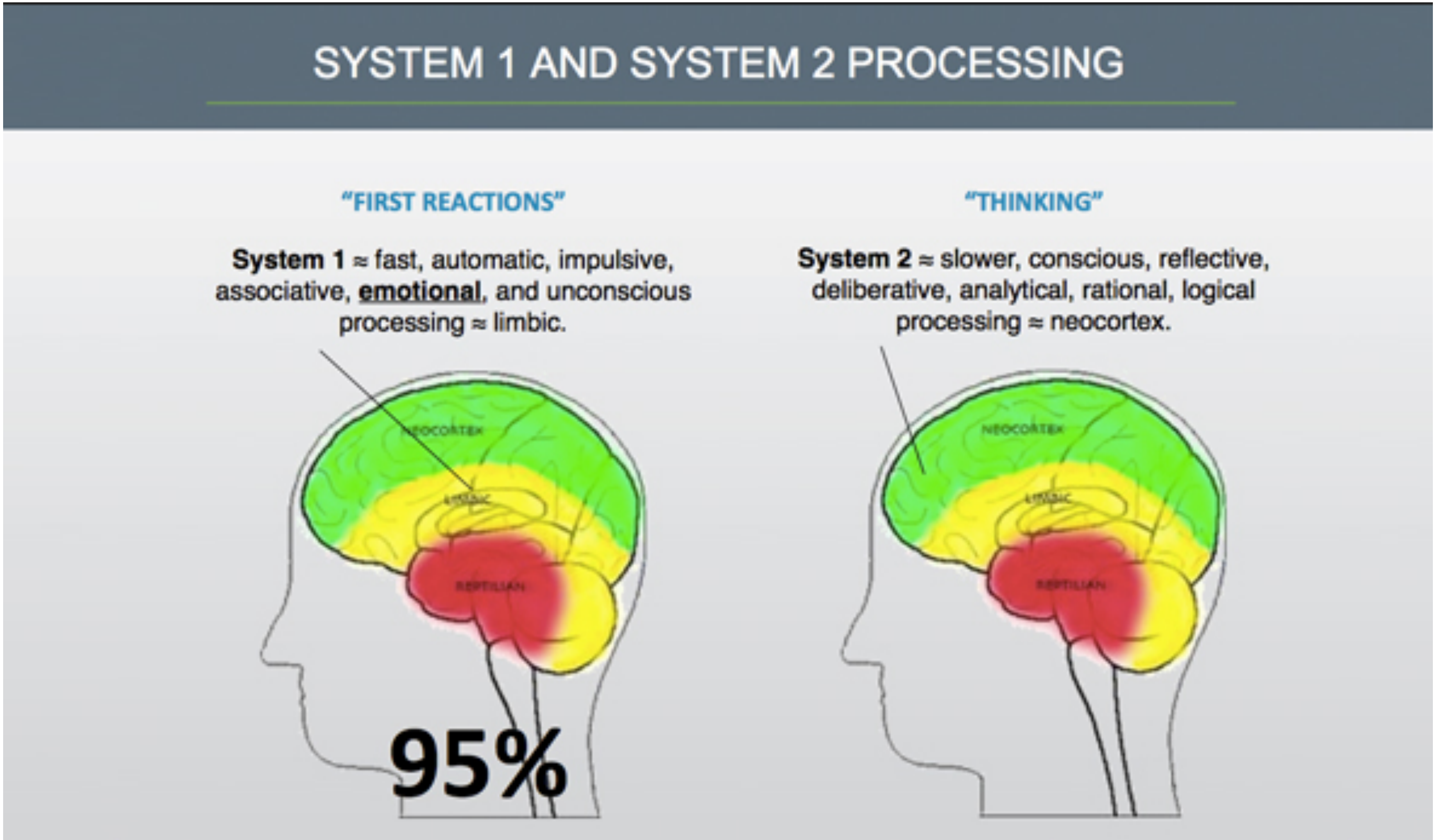


Quick – Solve **One** of These!



Our Brain Works on Auto-Pilot Sometimes…





SYSTEM 1 AND SYSTEM 2 PROCESSING

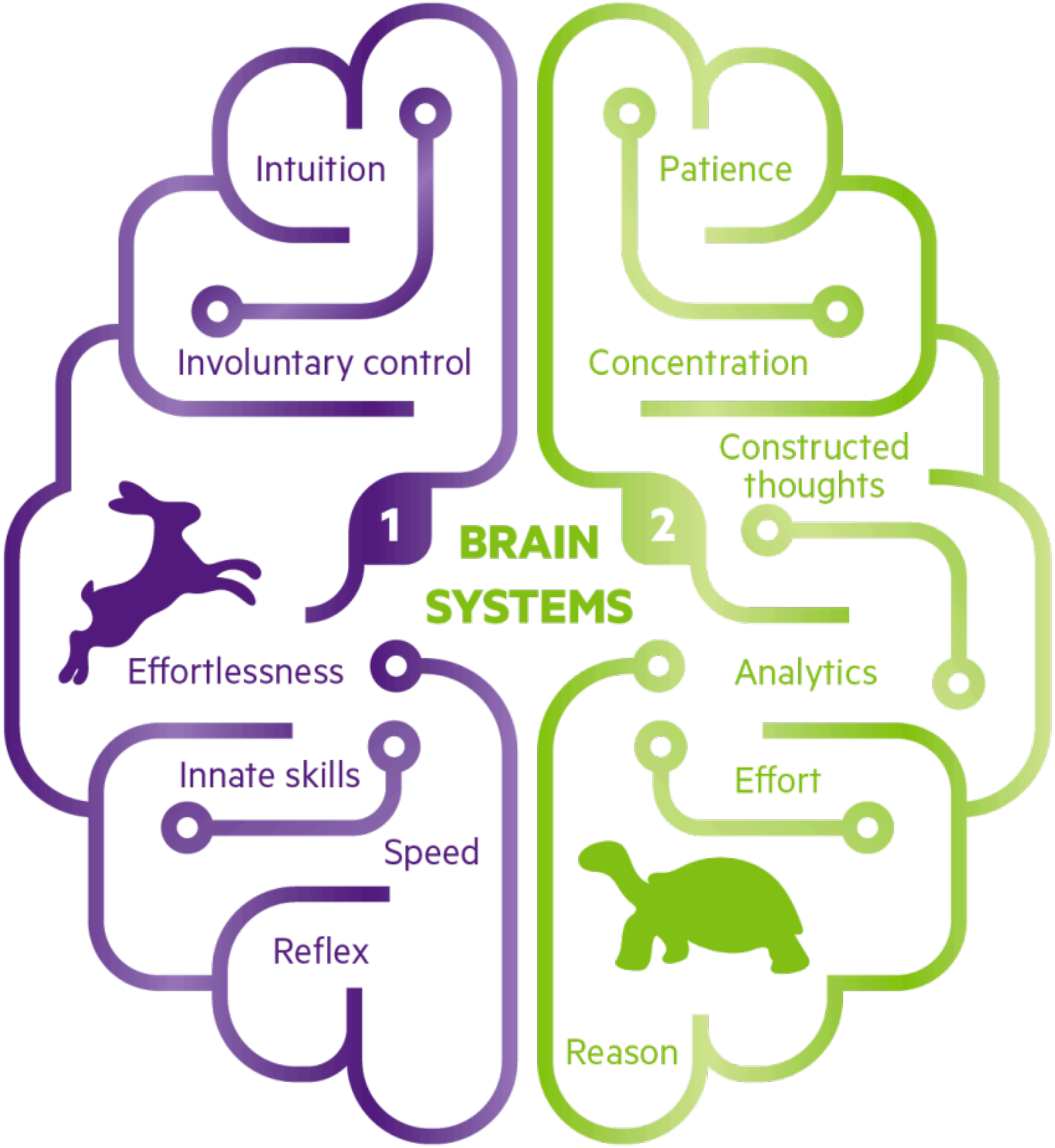
"FIRST REACTIONS"

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

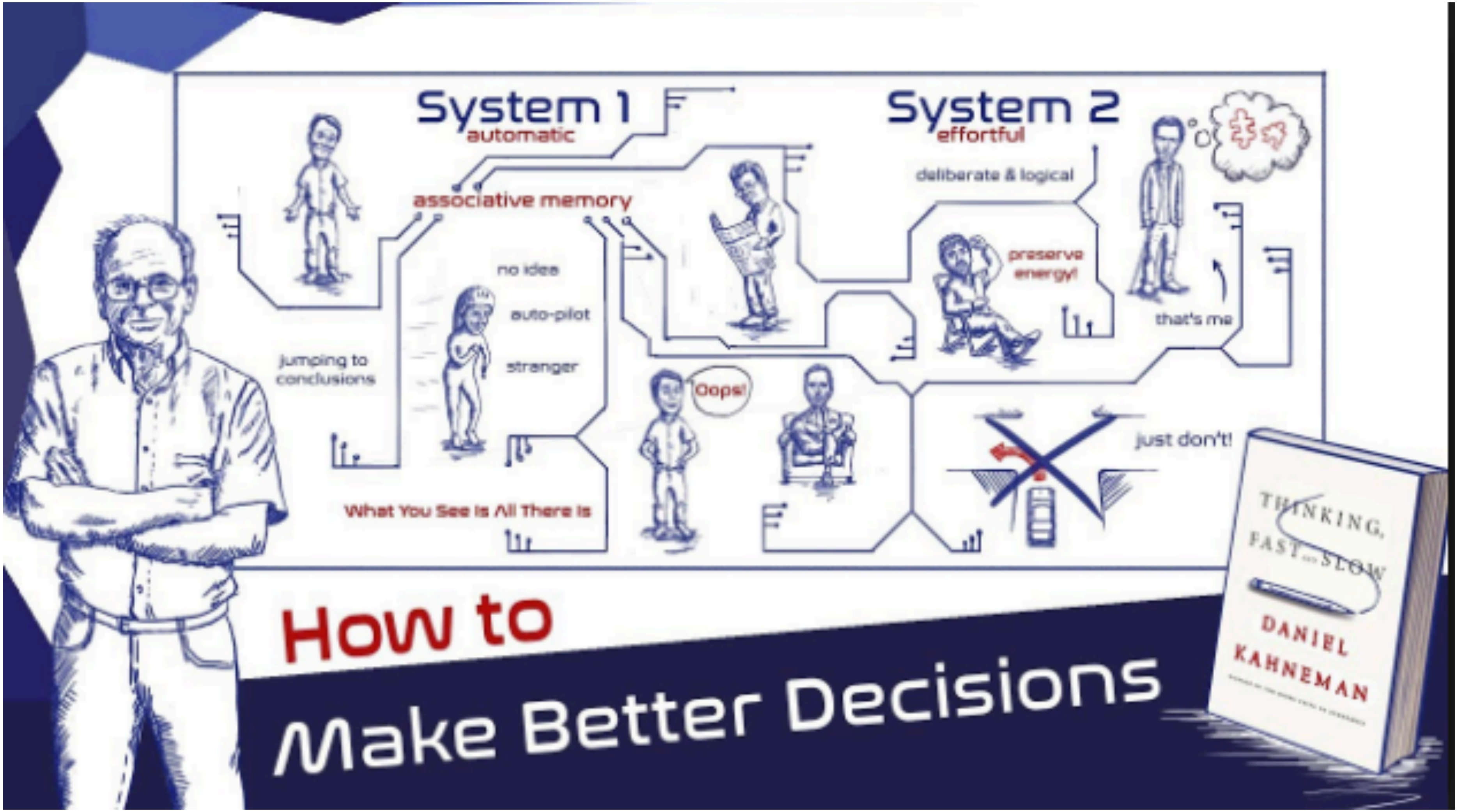
"THINKING"

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

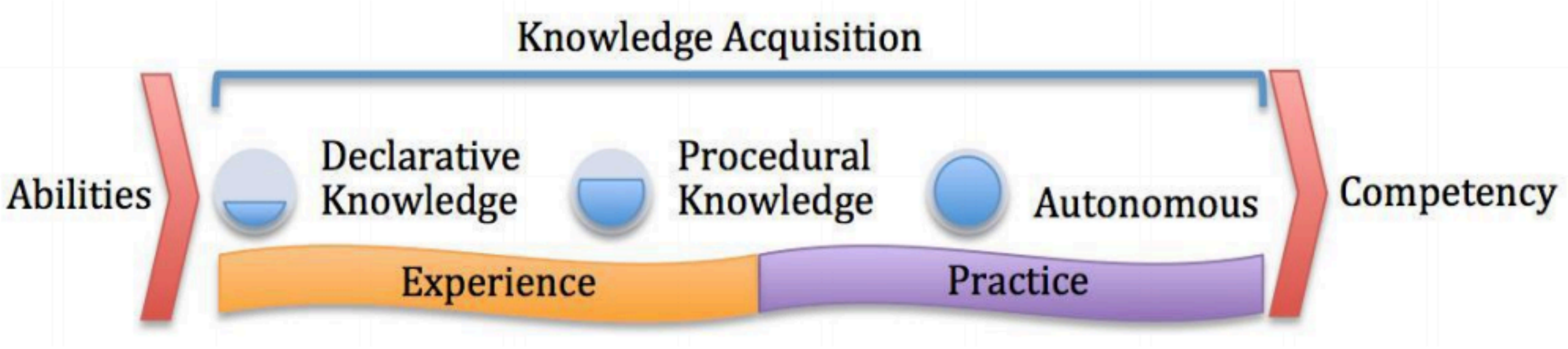
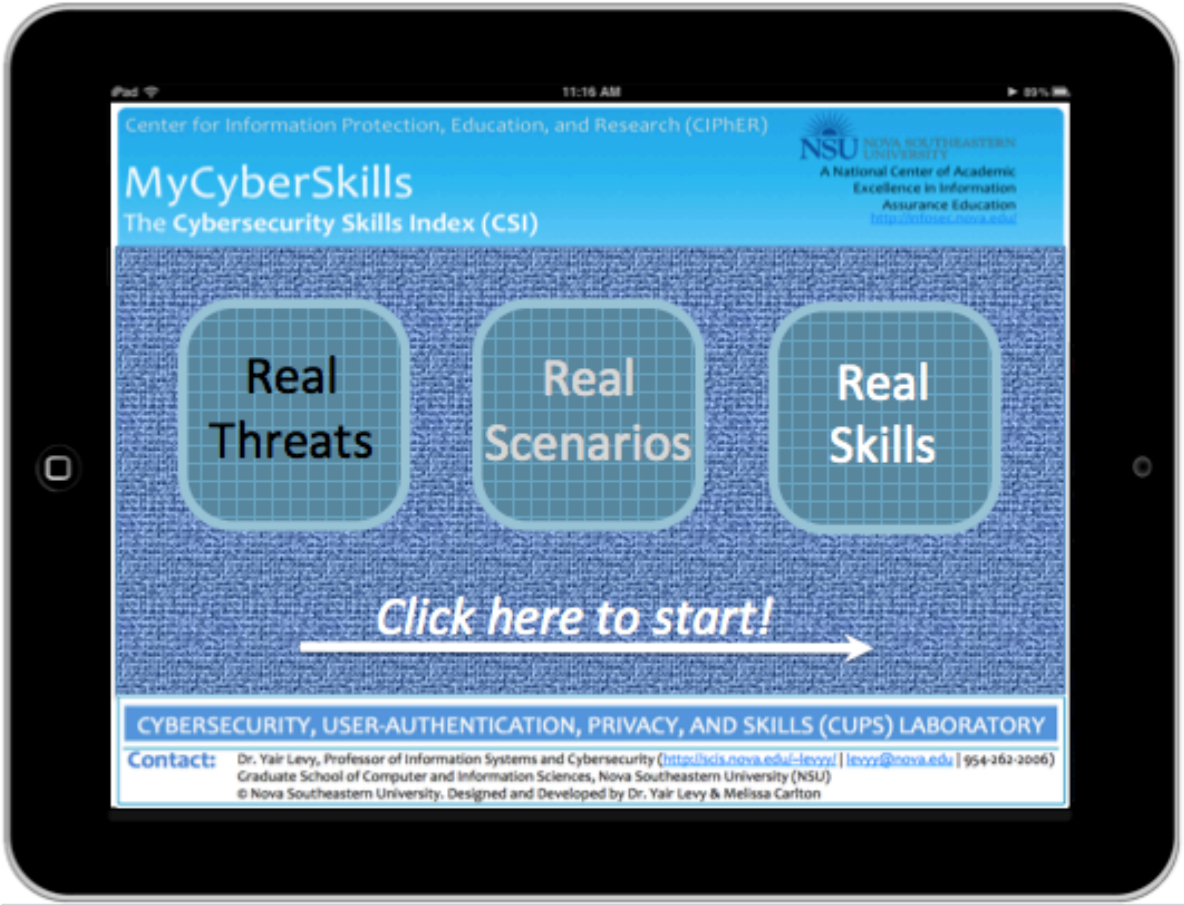


Figure 1. The Stages of Skill Development and Competency Attainment

Carlton, M., Levy, Y., & Ramim, M. M. (2019). Mitigating cyber attacks through the measurement of non-IT professionals' cybersecurity skills. Information and Computer Security, 27(1), 101-121. https://doi.org/10.1108/ICS-11-2016-0088

Carlton, M., Levy, Y., & Ramim, M. M. (2018). Validation of a vignettes-based, hands-on cybersecurity threats situational assessment tool. Online Journal of Applied Knowledge Management, 6(1), 107-118. https://doi.org/10.36965/OJAKM.2018.6(1)107-118

Measuring Cybersecurity Skills



Center for Information Protection, Education, and Research (CIPhER)

MyCyberSkills

The Cybersecurity Skills Index (CSI)

NSU NOVA SOUTHEASTERN UNIVERSITY

A National Center of Academic Excellence in Information Assurance Education

http://infosec.nova.edu/

Real Threats

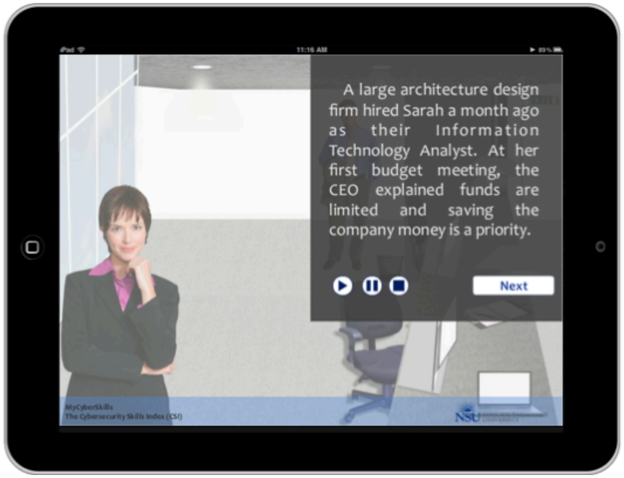
Real Scenarios

Real Skills

Click here to start!

CYBERSECURITY, USER-AUTHENTICATION, PRIVACY, AND SKILLS (CUPS) LABORATORY

Contact: Dr. Yair Levy, Professor of Information Systems and Cybersecurity (http://scis.nova.edu/~levyy/ | levyy@nova.edu | 954-262-2006)
Graduate School of Computer and Information Sciences, Nova Southeastern University (NSU)
© Nova Southeastern University. Designed and Developed by Dr. Yair Levy & Melissa Carlton

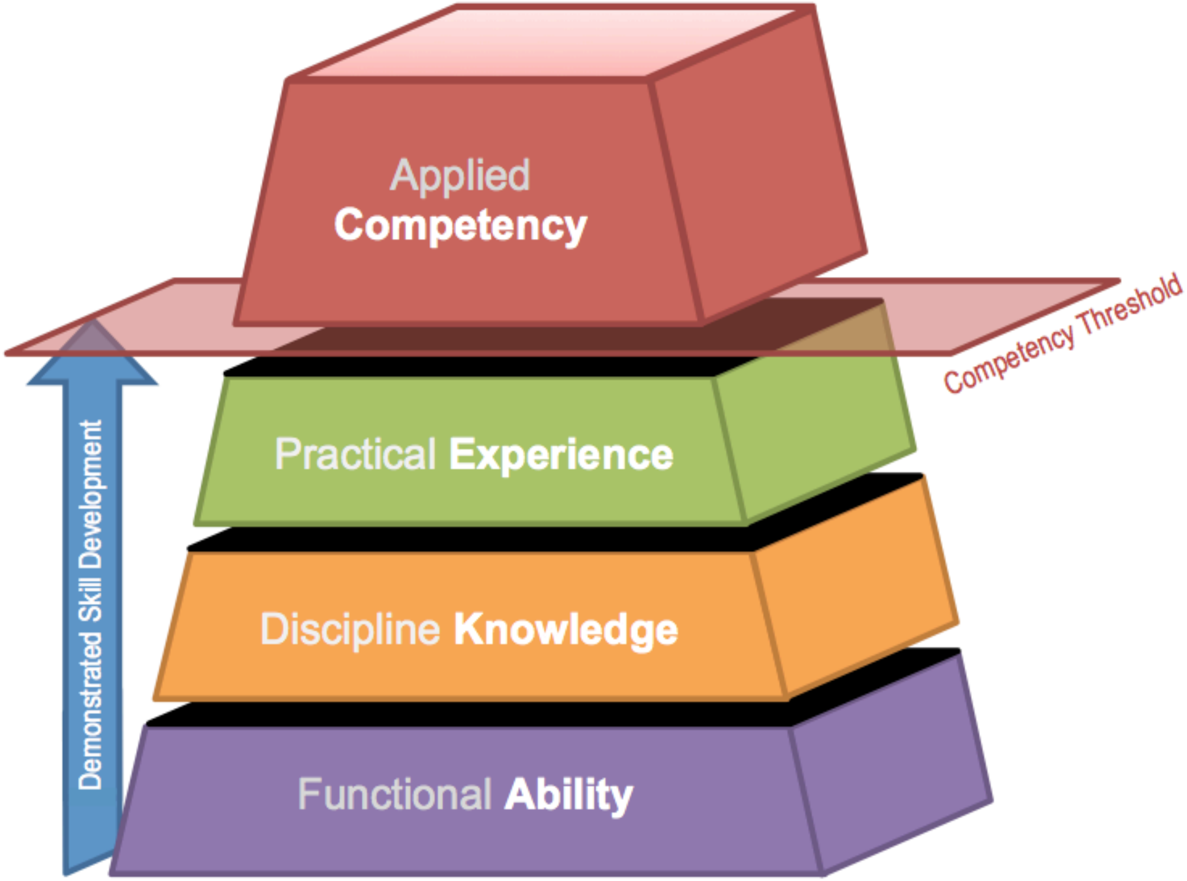


A large architecture design firm hired Sarah a month ago as their Information Technology Analyst. At her first budget meeting, the CEO explained funds are limited and saving the company money is a priority.

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*"

Cyber Situational vs. Curiosity as Measure of Risk

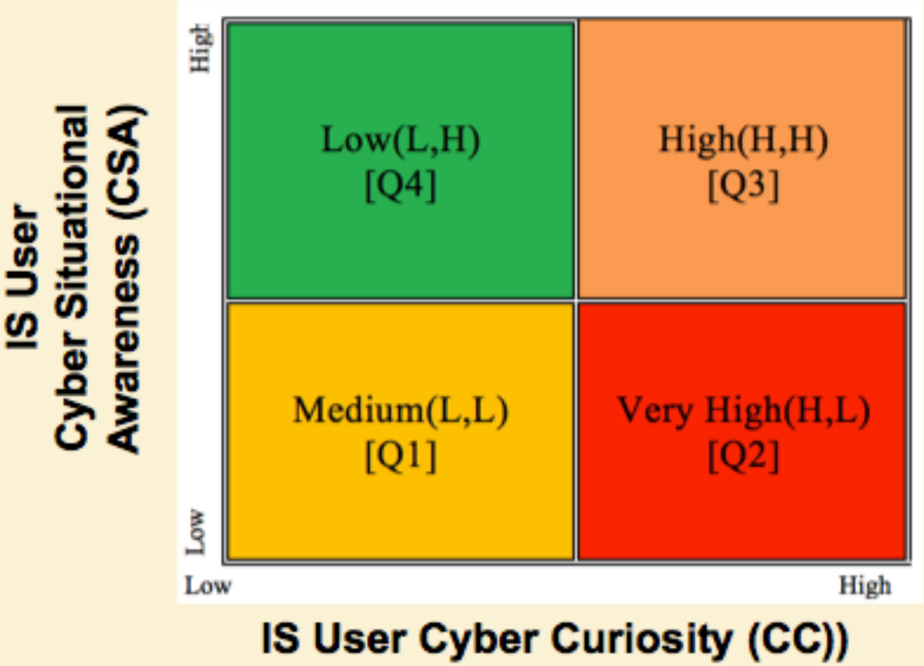


Figure 3 User cyber SA and cyber curiosity cyber risk taxonomy

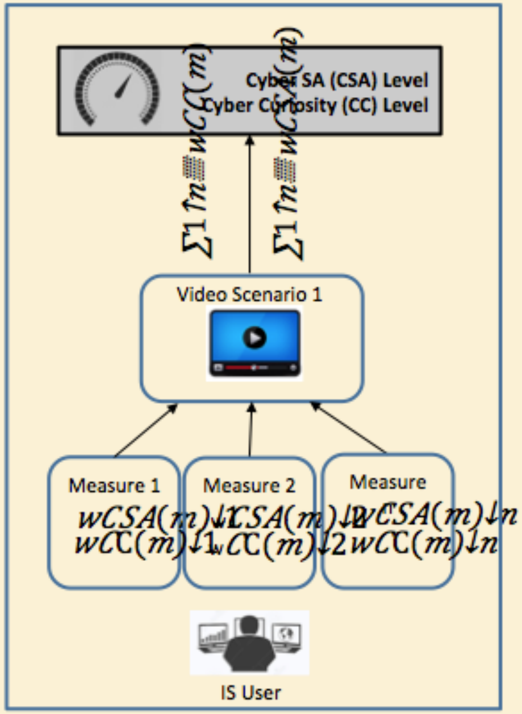


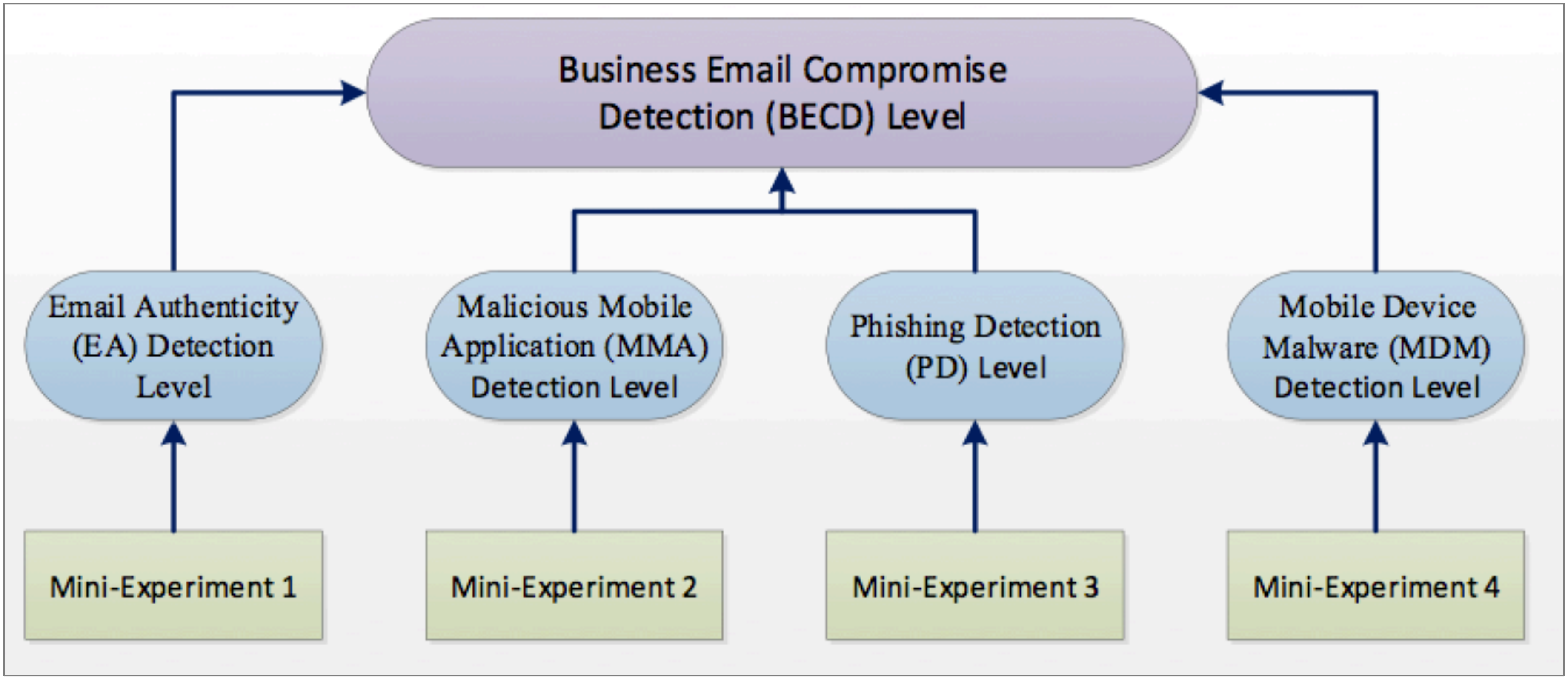
Figure 4. Conceptual design of the cyber SA and cyber curiosity measurement approach

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*"

Detecting Business E-mail Compromise (BEC)

http://becd.app/



Business Email Compromise Detection (BECD) Level

Email Authenticity (EA) Detection Level

Malicious Mobile Application (MMA) Detection Level

Phishing Detection (PD) Level

Mobile Device Malware (MDM) Detection Level

Mini-Experiment 1

Mini-Experiment 2

Mini-Experiment 3

Mini-Experiment 4

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

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

Types of Human Error in Large Data Breaches

OH SHOOT!

Price Waterhouse Coopers database

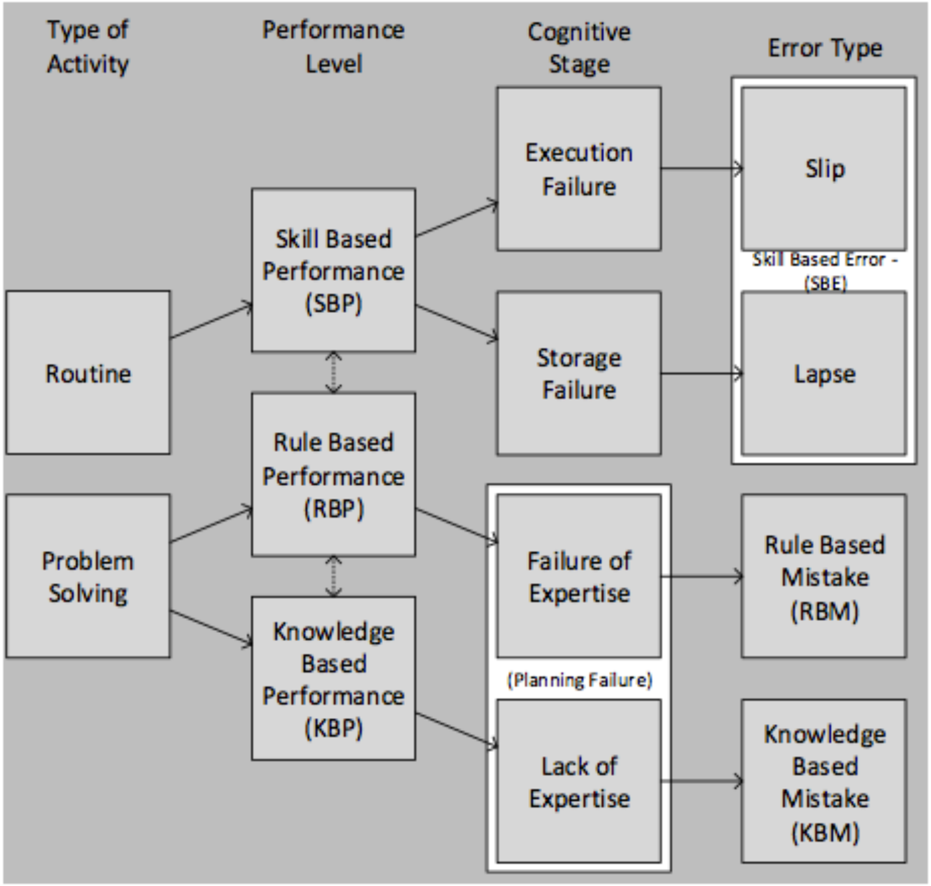
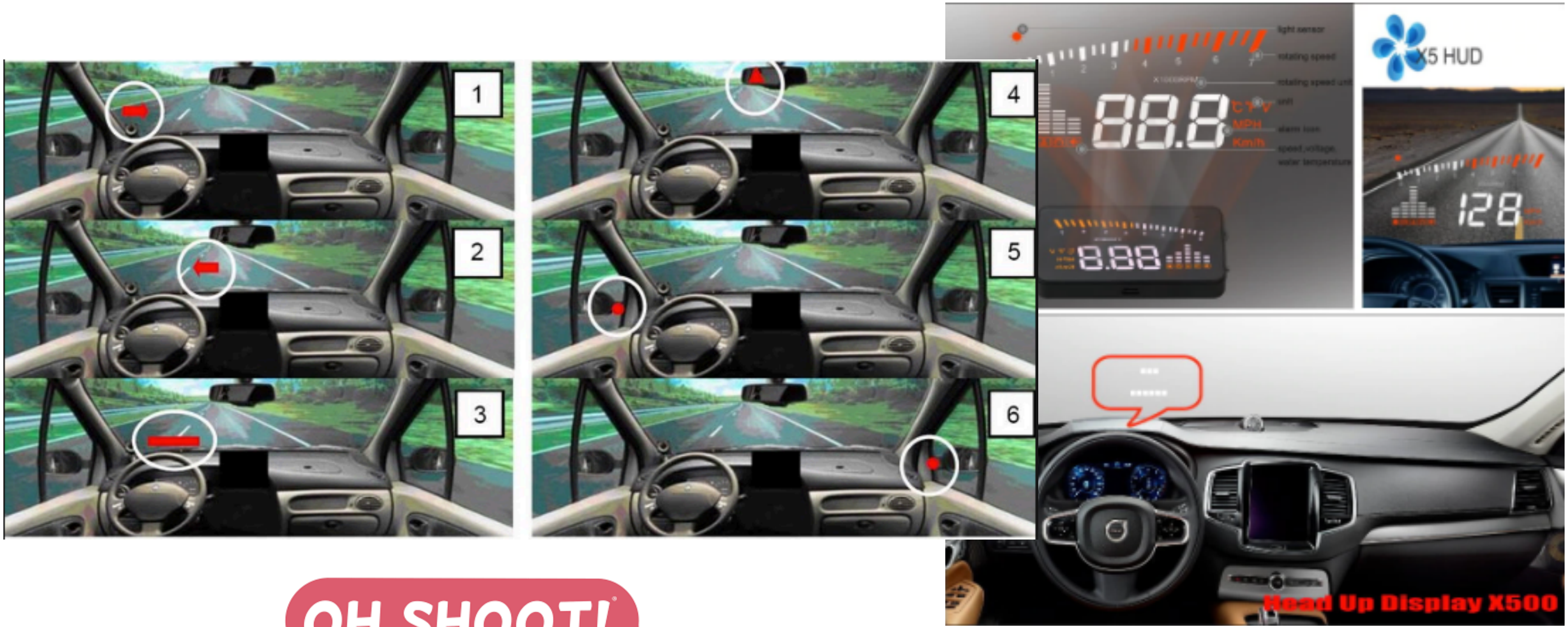


Figure 1: Generic Error-Modeling System (GEMS) adapted from Reason (1990)

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

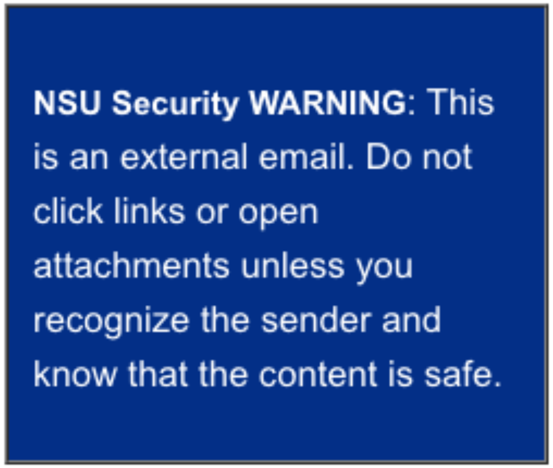
Audio, Visual, and Haptics Alerts and Warnings



Molly Cooper, Ph.D. - Assistant Professor - Ferris State University
Dissertation title: "*Assessment of Audio and Visual Warnings to Mitigate Risk of Phishing Attacks*"

Pause for a Cybersecurity Cause

The single-use timer that will wholesale for about a dollar is designed to make a nurse's life easier. Photo: David Tenenbaum


NSU Security WARNING: This is an external email. Do not click links or open attachments unless you recognize the sender and know that the content is safe.

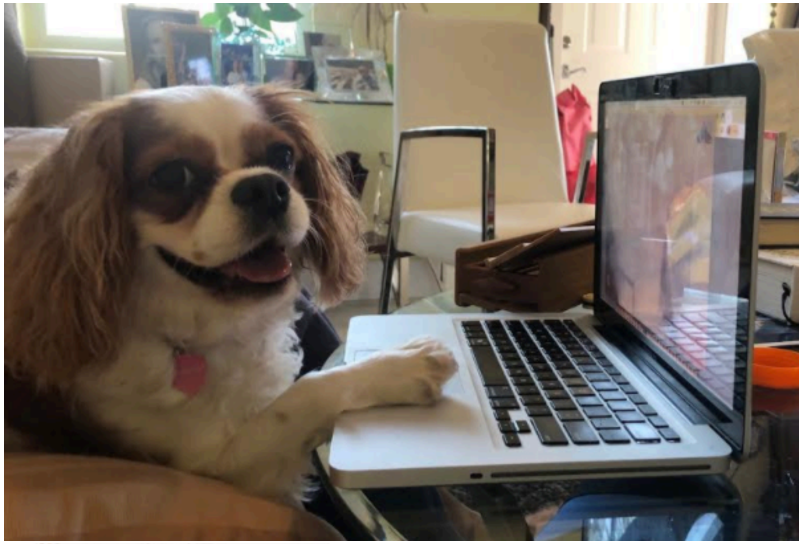
OH SHOOT!

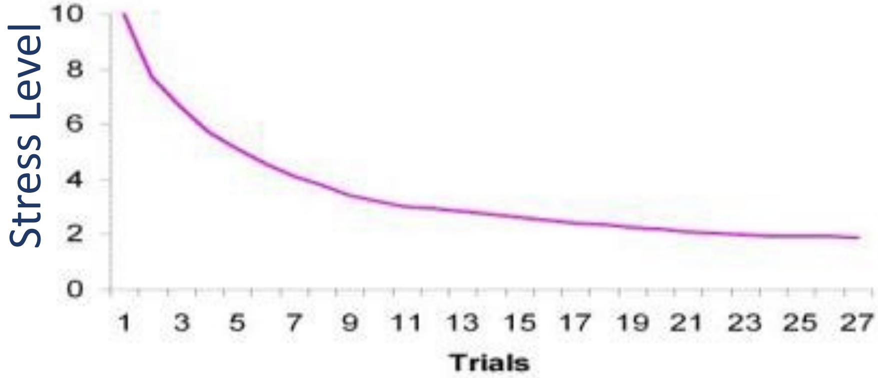
Amy Antonucci, Ph.D. Student

Dissertation title: *"Pause for a Cybersecurity Cause: Assessing the Influence of a Waiting Period on User Habituation in Mitigation of Phishing Attacks"*

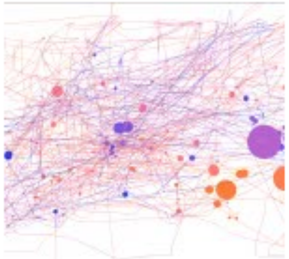
aa2539 AT mynsu.nova.edu

Static and Polymorphic Tactile Stimuli's Effect on Habituation





Eye Tracking



Mouse-cursor tracking

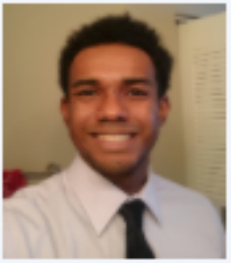
Javier Coto, Ph.D. Student

Dissertation title: *"An Empirical Investigation of Static and Polymorphic Tactile Stimuli's Effect on Habituation to Mitigate Malware Attack Vector"*

jc3379 AT mynsu.nova.edu

Cyber Risks to Organizations

Keiona Davis, Ph.D. Candidate
Dissertation title: "*The Role of Cybersecurity Responsibility in Small to Medium Enterprises (SMEs) on Risk of Point-of-Sale (POS) Data Breach*"
keiona AT mynsu.nova.edu



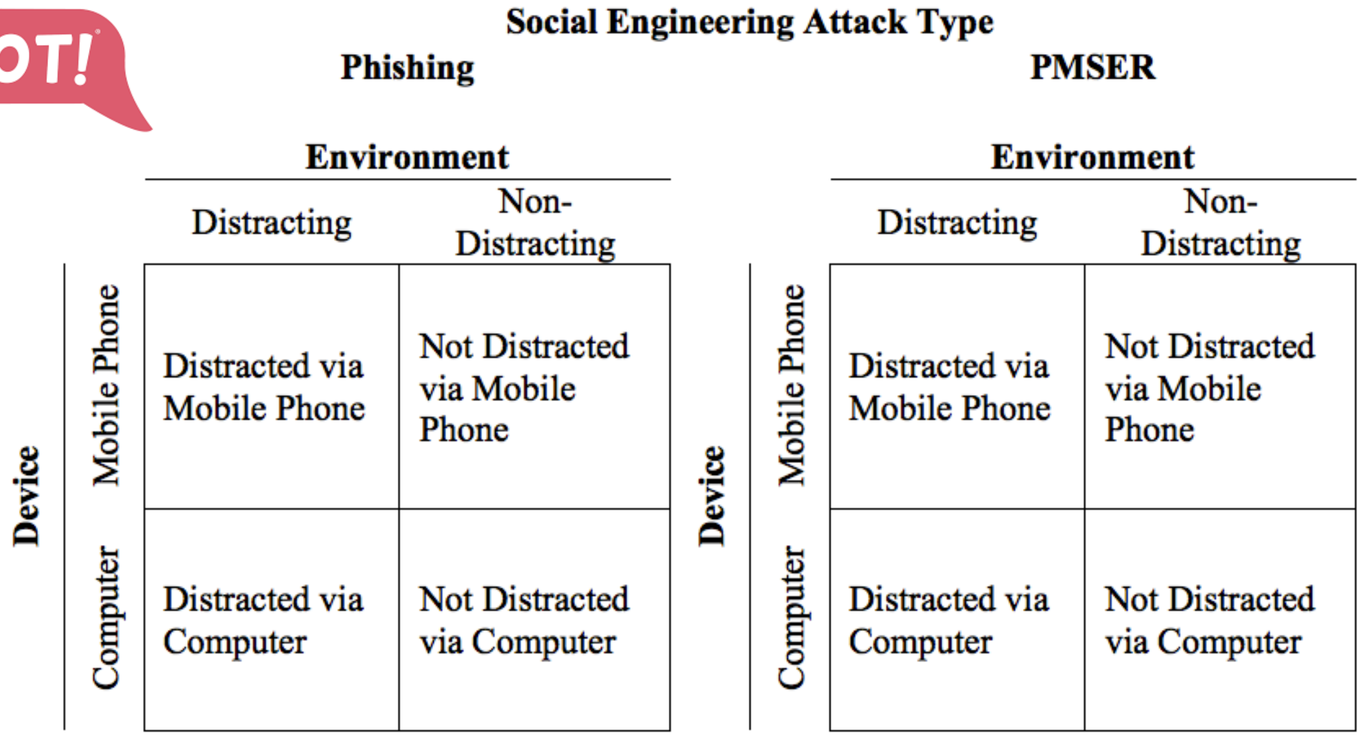
Emmanuel Jigo, Ph.D. Candidate
Dissertation title: "*Development of Criteria for Mobile Device Cybersecurity Threat Classification and Communication Standard using Labels, Pictogram, as well as Safety Data Sheets*"
ej459 AT mynsu.nova.edu

Andrea Di Fabio, Ph.D. Student
Dissertation title: "Development and Validation of a User Cyber Activity Risk Scoring Model Using Domain Name Category Ranking"
ad2045 AT mynsu.nova.edu

Patricia Baker, Ph.D. Student
Dissertation title: "*A Universal Cybersecurity Competency Framework for Organizational Users*"
patrbake AT mynsu.nova.edu

Judgment Errors: Environment & Device Type

OH SHOOT!



Social Engineering Attack Type

Phishing

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

PMSER

		Environment	
		Distracting	Non-Distracting
Device	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

Rationale for the Research

- Phishing continues to be an invasive threat to computer and mobile device users (McElwee et al., 2018).

- Deceptive search engine results pose a problem because cybercriminals often manipulate the results algorithms through search poisoning techniques, which promote malicious links to the first page of the search engine results (John et al., 2011; Leontiadis et al., 2014).

- Users of mobile phones, in particular, are more vulnerable to phishing attacks than those who use Personal Computers (PCs) due to poor fraudulent website detection of some mobile browsers along with the limitation of the smaller screen (Mavroeidis & Nicho, 2017; Tsalis et al., 2015; Virvilis et al., 2014).

Research Problem

The research problem that this study will address is financial losses to individuals and organizations due to phishing and malware/ransomware infection from emails, along with Potentially Malicious Search Engine Results (PMSER) (Anderson et al., 2013; Choo, 2011; Wright & Marett, 2010).

Cybercriminals use increasingly ingenious schemes to take advantage of users’ judgment errors when dealing with phishing emails and PMSER (Dhamija et al., 2006; Leontiadis et al., 2014).

Background

- Phishing scams are one of the oldest and widely used social engineering methods to gain personal information and infiltrate organizational systems, mainly for financial gain (Anderson et al., 2013; Marett & Wright, 2009; Moody et al., 2017).

- ***“Social engineering consists of persuasion techniques to manipulate people into performing actions or divulging confidential information”*** (Ferreira et al., 2015, p. 36).

- Phishing attempts often are email-based attacks but can also occur through spoofed website links (Vishwanath et al., 2011; Zhao et al., 2017).

Background (Cont.)

- Environmental factors affect the way that users perform tasks in the workplace, at home, and in public (Dalton & Behm, 2007; Kallinen, 2004; Vredeveldt & Perfect, 2014). ***Background noise*** tends to have a negative effect on task performance because it distracts and interrupts users (Dalton & Behm, 2007; Larsby et al., 2008). The use of background music, however, has mixed results (Dalton & Behm, 2007; Kallinen, 2004).

- ***Distracting environments*** can have a negative effect on working and attentional memory (Awh & Jonides, 2001; Rodrigues & Pandeirada, 2015). Lapses of attention caused by external distractions interrupt task performance by inhibiting the attentive processes of working memory (Berti & Schröger, 2001; Christophel et al., 2017).

- Rodrigues and Pandeirada (2015) tested the working memory in 40 elderly research participants in distracting and non-distracting environments and found that they performed the tasks better in the non-distracting environment.

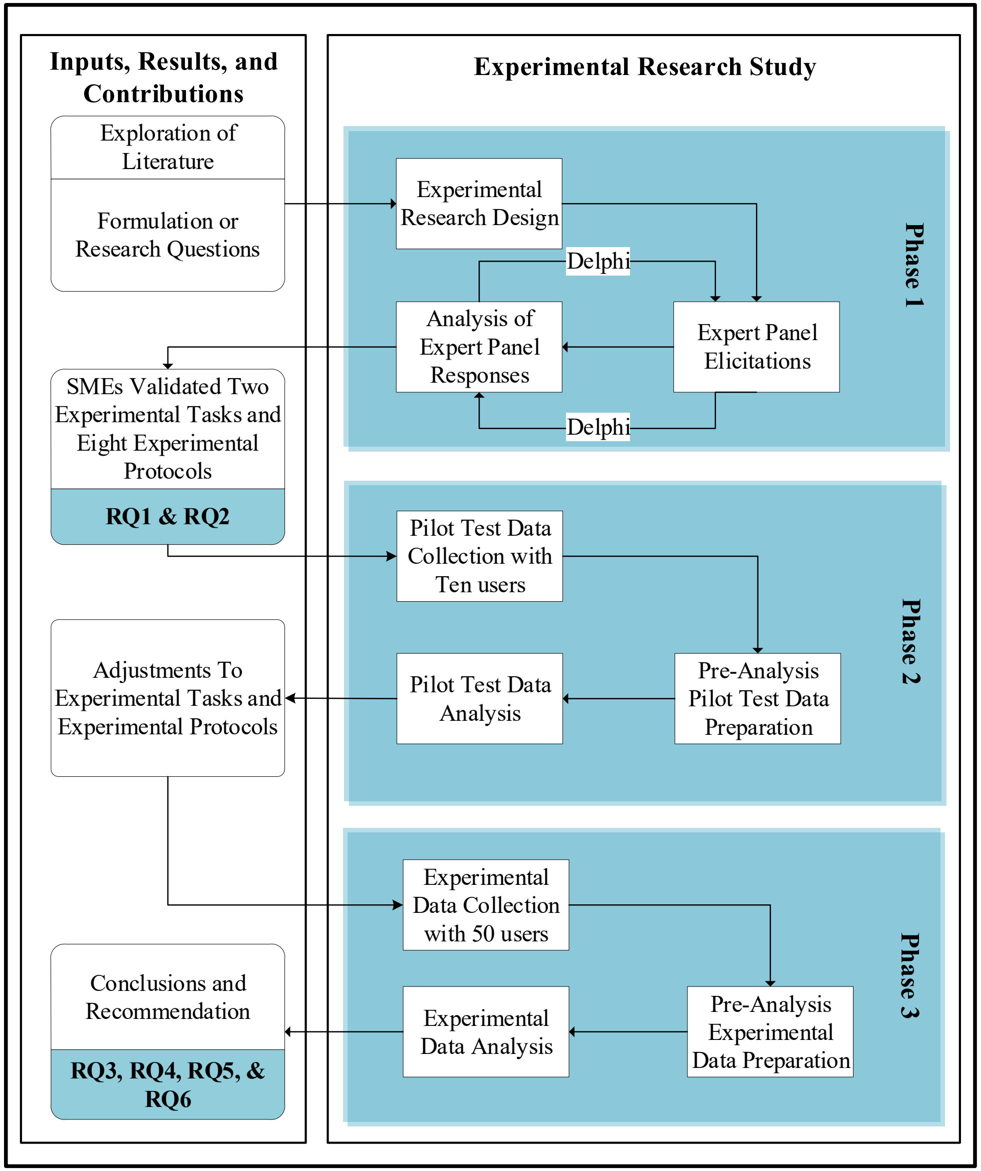
Background (Cont.)

- Many researchers have studied the reasons that humans make choices when faced with decisions often under uncertain terms (Fox & Tversky, 1998; Kahneman & Tversky, 1982; Tversky & Kahneman, 1992).

- Some of these choices are reason-based, belief-based, and can involve bias (Ayton & Pascoe, 1995; Fox & Tversky, 1998; Shafir et al., 1993).

- ***Human error*** has been researched for decades by several researchers that have made extensive contributions to other research fields (Cohen, 1981; Reason, 1990; Tversky & Kahneman, 1974, 1983).

Methodology - Experimental Field Study



Inputs, Results, and Contributions
Exploration of Literature
Formulation or Research Questions
SMEs Validated Two Experimental Tasks and Eight Experimental Protocols
RQ1 & RQ2
Adjustments To Experimental Tasks and Experimental Protocols
Conclusions and Recommendation
RQ3, RQ4, RQ5, & RQ6
Experimental Research Study
Phase 1
Experimental Research Design
Delphi
Analysis of Expert Panel Responses
Expert Panel Elicitations
Delphi
Phase 2
Pilot Test Data Collection with Ten users
Pilot Test Data Analysis
Pre-Analysis Pilot Test Data Preparation
Phase 3
Experimental Data Collection with 50 users
Experimental Data Analysis
Pre-Analysis Experimental Data Preparation

This Research Study Design

This part of the research has six specific goals:

1. To identify and validate, using subject matter experts (SMEs), *two sets of experimental tasks* for the measures of users' judgment when exposed to two types of simulated social engineering attacks (phishing & PMSER).

2. To identify and validate, using SMEs, *eight experimental protocols* to assess the measures of users' judgment when exposed to two types of simulated social engineering attacks (phishing & PMSER).

3. To find if there are any statistically significant mean differences in users’ judgment when exposed to two types of simulated social engineering attacks (phishing & PMSER).

This Research Study Design (Cont.)

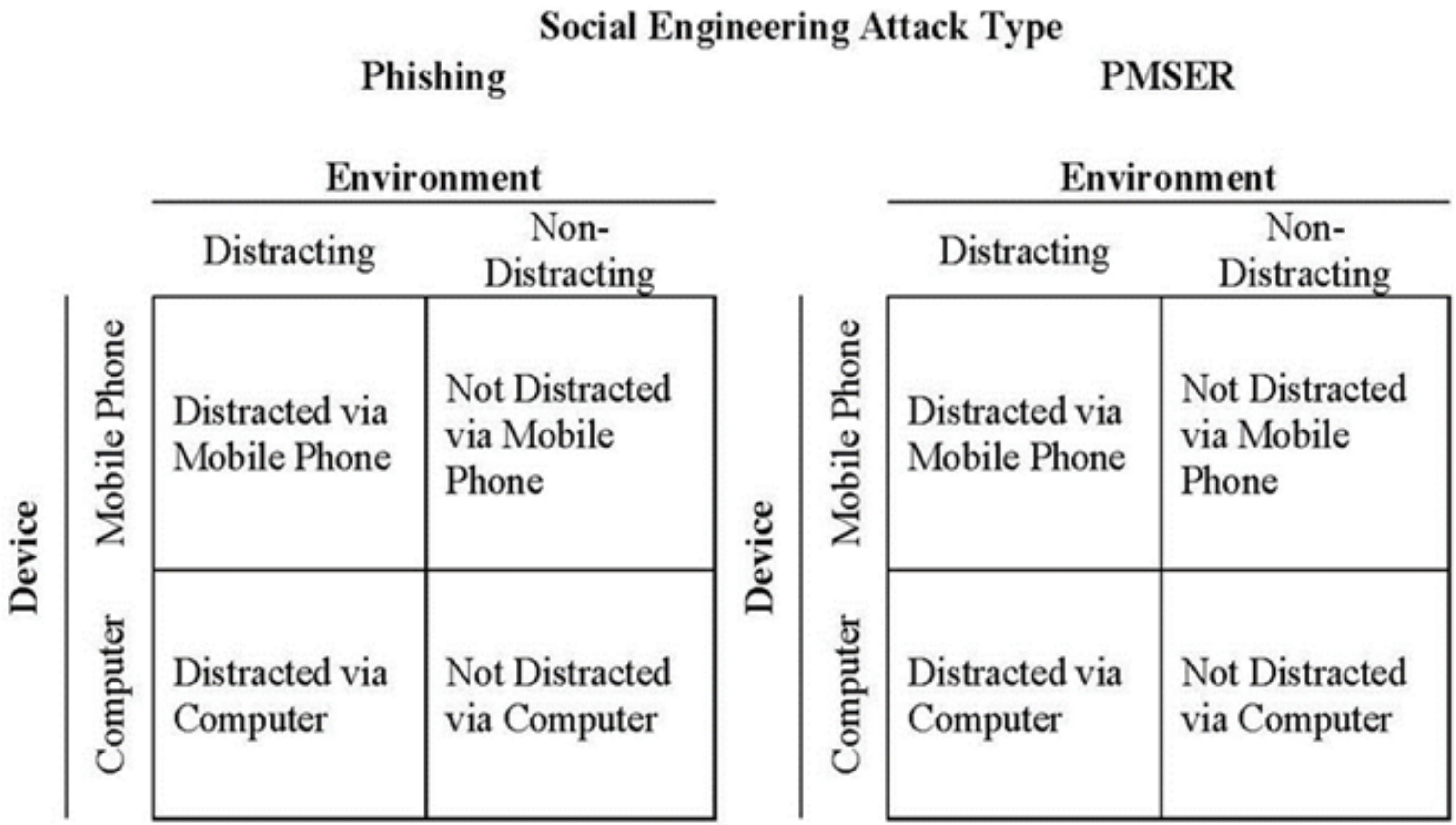
4. To find if there are any statistically significant mean differences in users’ judgment when exposed to two types of simulated social engineering attacks (phishing & PMSER).

5. To find if there are any statistically significant mean differences in users’ judgment when exposed to two types of simulated social engineering attacks (phishing & PMSER) based on the interaction of the types of environment and type of device used.

6. To find if there are any statistically significant mean differences in users’ judgment when exposed to two types of simulated social engineering attacks (phishing & PMSER), when controlled for the users’: (a) gender, (b) age, (c) education, and (d) level of social media usage.

Phishing and PMSER IQ Mini Tests

Eight sets of mini IQ tests will be created based on the environment and the device type



Social Engineering Attack Type

Phishing

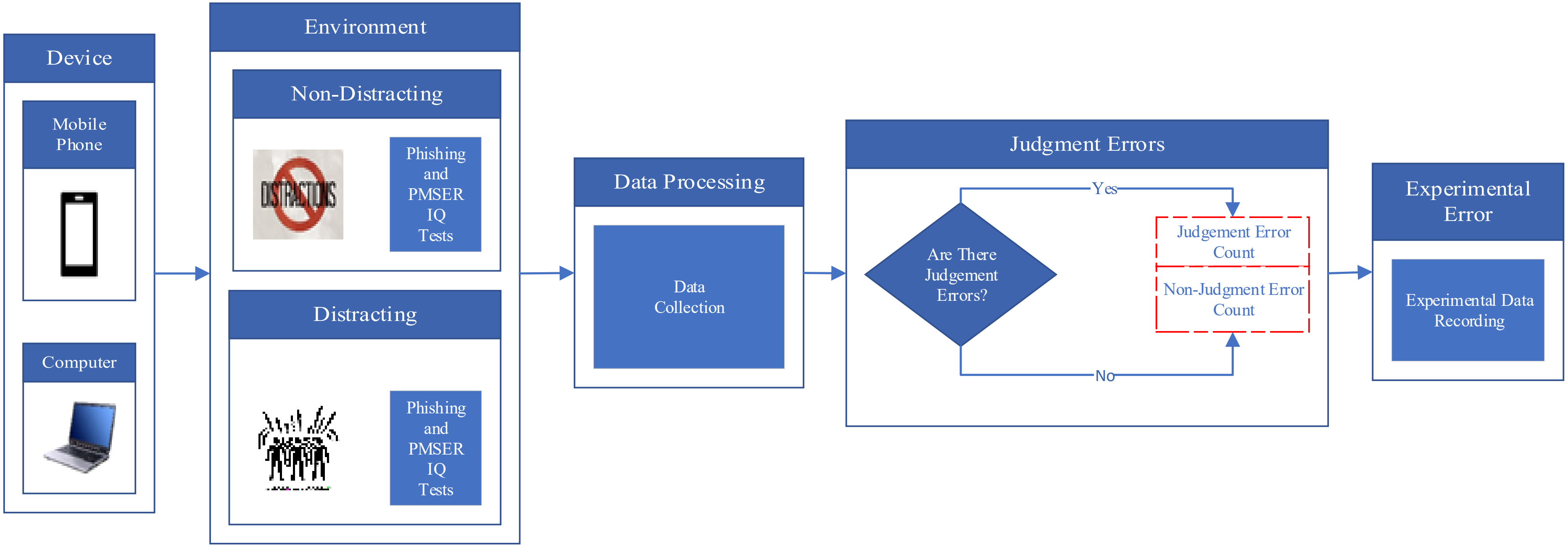
		Environment	
		Distracting	Non-Distracting
Device	Mobile Phone	Distracted via Mobile Phone	Not Distracted via Mobile Phone
	Computer	Distracted via Computer	Not Distracted via Computer

PMSER

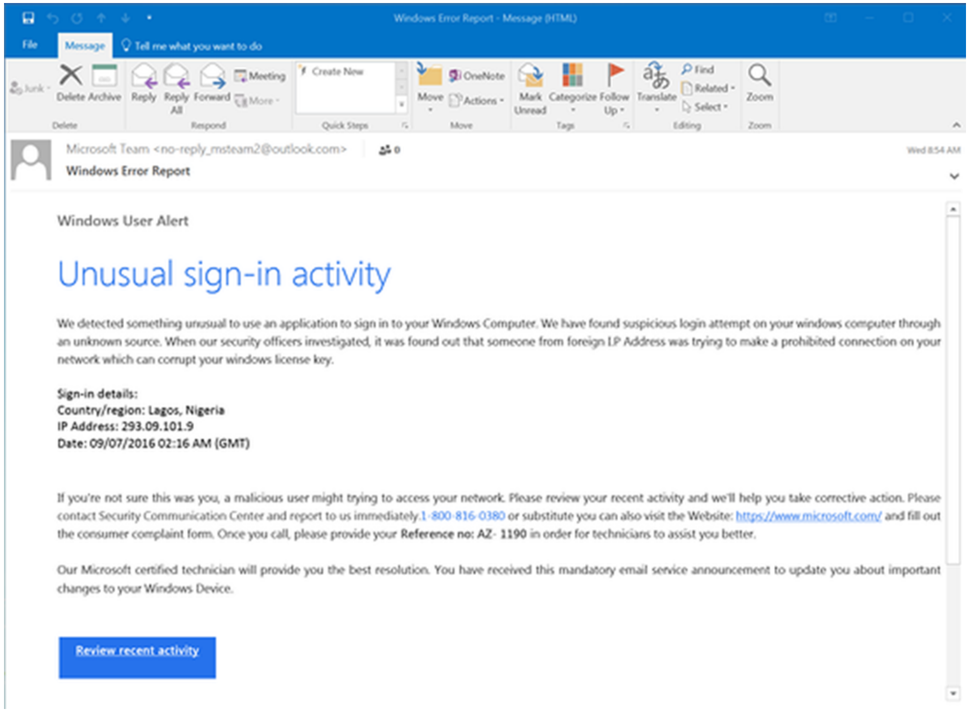
		Environment	
		Distracting	Non-Distracting
Device	Mobile Phone	Distracted via Mobile Phone	Not Distracted via Mobile Phone
	Computer	Distracted via Computer	Not Distracted via Computer

Phishing and PMSER Experimental Tasks

Experimental Tasks for the Measures of Users' Judgment When Exposed to Two Types of Simulated Social Engineering Attacks (Phishing & PMSER).



Phishing IQ Test Examples



Microsoft Team <no-reply_msteam2@outlook.com>

Windows Error Report

Wed 8:54 AM

Windows User Alert

Unusual sign-in activity

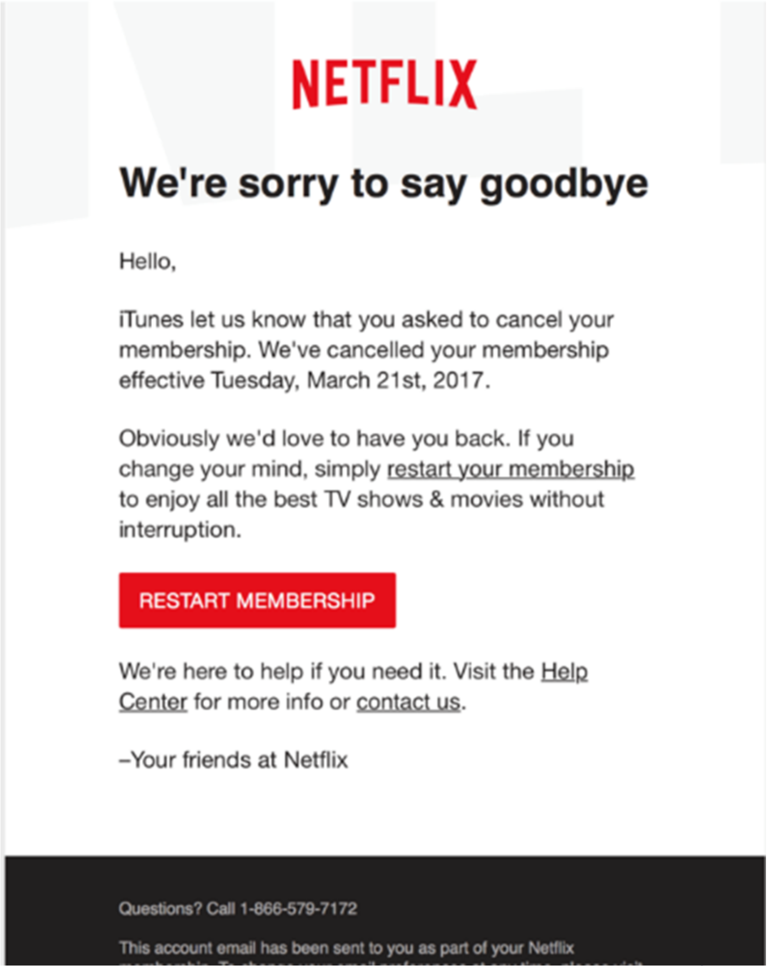
We detected something unusual to use an application to sign in to your Windows Computer. We have found suspicious login attempt on your windows computer through an unknown source. When our security officers investigated, it was found out that someone from foreign I.P Address was trying to make a prohibited connection on your network which can corrupt your windows license key.

Sign-in details:
Country/region: Lagos, Nigeria
IP Address: 293.09.101.9
Date: 09/07/2016 02:16 AM (GMT)

If you're not sure this was you, a malicious user might trying to access your network. Please review your recent activity and we'll help you take corrective action. Please contact Security Communication Center and report to us immediately.1-800-816-0380 or substitute you can also visit the Website: https://www.microsoft.com/ and fill out the consumer complaint form. Once you call, please provide your **Reference no: AZ- 1190** in order for technicians to assist you better.

Our Microsoft certified technician will provide you the best resolution. You have received this mandatory email service announcement to update you about important changes to your Windows Device.

Review recent activity



NETFLIX

We're sorry to say goodbye

Hello,

iTunes let us know that you asked to cancel your membership. We've cancelled your membership effective Tuesday, March 21st, 2017.

Obviously we'd love to have you back. If you change your mind, simply restart your membership to enjoy all the best TV shows & movies without interruption.

RESTART MEMBERSHIP

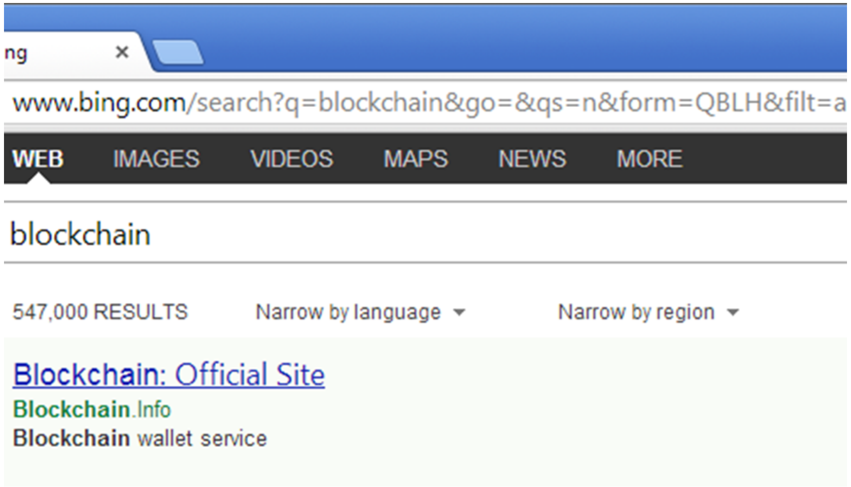
We're here to help if you need it. Visit the Help Center for more info or contact us.

–Your friends at Netflix

Questions? Call 1-866-579-7172

This account email has been sent to you as part of your Netflix

PMSER IQ Test Examples (Cont.)

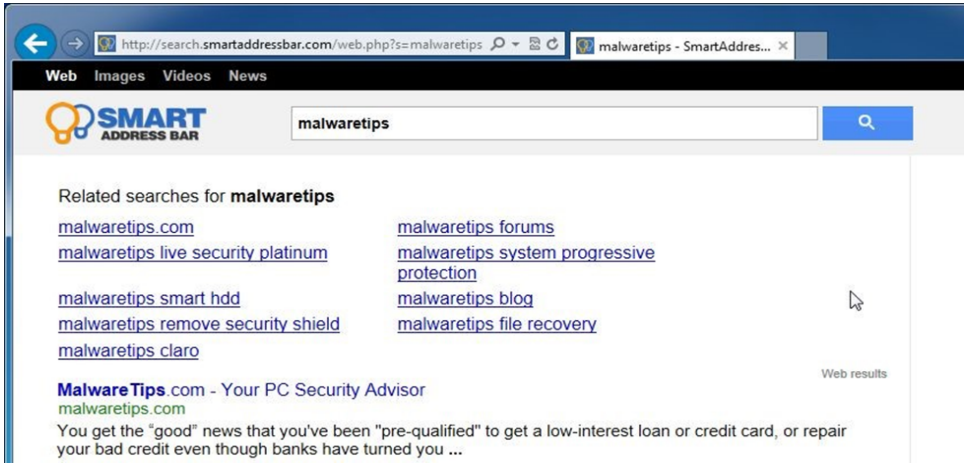


www.bing.com/search?q=blockchain&go=&qs=n&form=QBLH&filt=a

blockchain

547,000 RESULTS Narrow by language Narrow by region

Blockchain: Official Site
Blockchain.Info
Blockchain wallet service



http://search.smartaddressbar.com/web.php?s=malwaretips

malwaretips

Related searches for **malwaretips**

malwaretips.com	malwaretips forums
malwaretips live security platinum	malwaretips system progressive protection
malwaretips smart hdd	malwaretips blog
malwaretips remove security shield	malwaretips file recovery
malwaretips claro	

MalwareTips.com - Your PC Security Advisor
malwaretips.com
You get the "good" news that you've been "pre-qualified" to get a low-interest loan or credit card, or repair your bad credit even though banks have turned you ...

Phishing and PMSER SME Survey

Physical Environment and Audio/Visual (AV) Distraction Levels

- SMEs will be asked to rank their top choice of distracting and non-distracting physical environments along with AV distraction levels

Phishing and PMSER SME Survey (Cont.)

Physical Environment	AV Distraction Levels
Airport	Continuous Background Noise
Coffee Shop	Visual Distractions
Lecture Hall	Distracting/Loud Music
Meeting	Quiet Environment
Office Setting	Relaxing Background Music
Home	No Visual Distractions
Hotel Room	
Library/Bookstore	

Live Poll – Seeking Your Feedback!

Phishing and PMSER SME Survey (Physical Environment)

Which physical environment provides the **most distracting environment** for Mobile Phones and Computers?

A. Airport
B. Coffee Shop
C. Lecture Hall
D. Meeting

Live poll 1

Phishing and PMSER SME Survey (Physical Environment, cont.)

Which physical environment provides **the least distracting environment** for Mobile Phones and Computers?

A. Office Setting
B. Home
C. Hotel room
D. Library/Bookstore

Live poll 2

Phishing and PMSER SME Survey (Audio/Visual Distraction Levels)

Which audio/visual ***distraction level is best for a distracting environment*** for Mobile Phones and Computers?

A. Continuous Background Noise
B. Visual Distractions
C. Distracting/Loud Music
D. All of the above

Live poll 3

Phishing and PMSER SME Survey (Audio/Visual Distraction Levels, cont.)

Which audio/visual ***distraction level is best for a non-distracting environment*** for Mobile Phones and Computers?

A. A Quiet Environment
B. Relaxing Background Music
C. No visual distractions
D. All of the above

Live poll 4

Phishing and PMSER SME Survey (Cont.)

Sample emails and search engine results.

- SMEs will also be asked their opinion of sample emails and search engine results on whether to (a) ***keep***; (b) ***modify***; (c) ***replace*** each sample.
- These validated samples will be used in the research design process for each of the two experimental tasks and eight research protocols.

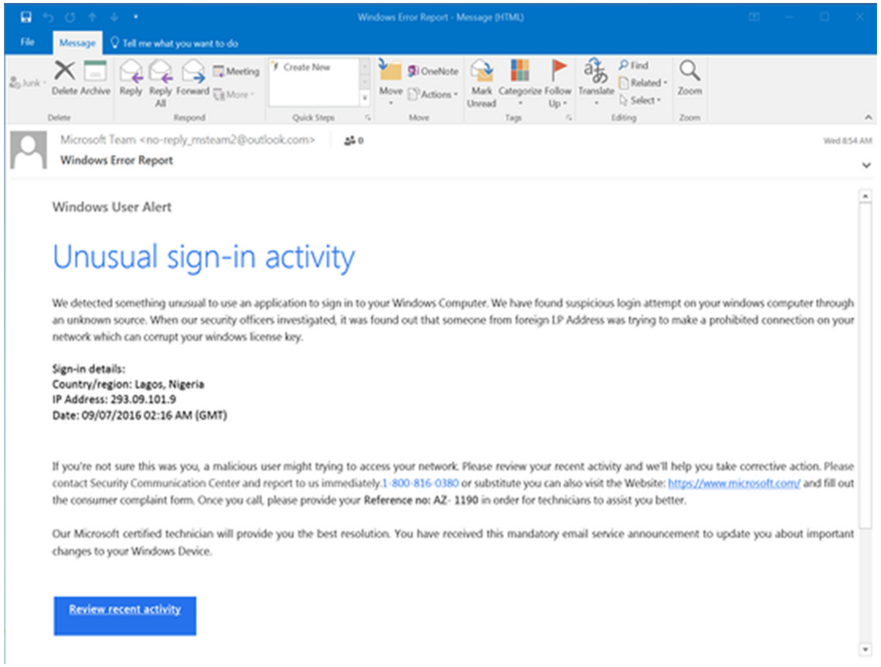
Phishing and PMSER SME Survey (Cont.)

- Data collected in the SMEs survey will be used to create eight mini IQ tests based on the:
  a) Environment
  b) Device Type

- Future research will also include a qualitative and quantitative data collection with participants through an application delivery system

Phishing and PMSER SME Survey (Cont.)

The following is a sample email that will be used for testing the experimental research study users if the email is legitimate, phishing, or ask the IT department. Do we keep this sample, revise it, or remove it?



Microsoft Team <no-reply_msteam2@outlook.com>

Wed 8:54 AM

Windows Error Report

Windows User Alert

Unusual sign-in activity

We detected something unusual to use an application to sign in to your Windows Computer. We have found suspicious login attempt on your windows computer through an unknown source. When our security officers investigated, it was found out that someone from foreign I.P Address was trying to make a prohibited connection on your network which can corrupt your windows license key.

Sign-in details:
Country/region: Lagos, Nigeria
IP Address: 293.09.101.9
Date: 09/07/2016 02:16 AM (GMT)

If you're not sure this was you, a malicious user might trying to access your network. Please review your recent activity and we'll help you take corrective action. Please contact Security Communication Center and report to us immediately.1-800-816-0380 or substitute you can also visit the Website: https://www.microsoft.com/ and fill out the consumer complaint form. Once you call, please provide your **Reference no: AZ- 1190** in order for technicians to assist you better.

Our Microsoft certified technician will provide you the best resolution. You have received this mandatory email service announcement to update you about important changes to your Windows Device.

Review recent activity

A. Keep

B. Revise

C. Replace

Discussion and Conclusions

- With the widespread use of mobile phones with Internet-connected applications, phishing attempts have increased through the use of social engineering through scams and clickbait links (Frauenstein & Flowerday, 2016; Halevi et al., 2013; Marett & Wright, 2009).

- Users pick up bad habits through the use of link sharing applications that leave them vulnerable to phishing attacks.

- Distracting environments at work and in public make it easier for users to have errors in judgment when performing tasks (Groff et al., 1983; Reason, 1995; Sanders & Baron, 1975).

Discussion and Conclusions (Cont.)

- Attackers craft phishing attacks to try and distort the mental model that users form in interacting with online transactions, to distract them from the visual cues that they would usually pick up on (Downs et al., 2006).

- As the number of distractions increases, cognitive cues decrease, affecting decision making due to cognitive overload (Groff et al., 1983; Kahneman, 1973; Speier et al., 1999).

- The results of this study will provide input to the body of knowledge (BoK) on users' susceptibility to social engineering attacks in distracting vs. non-distracting environments while using mobile phones vs. computers.

Future Work

- Future research will use the validated set of experiments to collect and analyze data to find if any significant mean differences exist in users' judgment when exposed to two types of simulated social engineering attacks (phishing & PMSER) and the two types of distracting environments while using mobile phones or desktop/laptop computers.

- Prior literature indicated that various demographic indicators such as age, gender, education, and level of social media usage, also play a role in phishing judgmental errors (Frauenstein & Flowerday, 2016; Sheng et al., 2010). As such, additional assessments of the experimental data with the interaction of the different demographic indicators may help further uncover potential groups that are more susceptive to social engineering attacks.

Would you like to participate in the SMEs survey?

Please email Tommy Pollock at:
tp809@mynsu.nova.edu

Thank you!

NSU
Florida

NOVA SOUTHEASTERN
UNIVERSITY

Center for Information Protection, Education, and Research (CIPhER):

https://infosec.nova.edu/

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