NSUComputing

# Inaugural Cybersecurity Graduate Research Symposium

**October 11, 2023**

**10am - 4:30pm**

**Nova Southeastern University - Cortex Labs Rm 309, Mailman Hollywood Building**

SCAN ME

National Center of Academic Excellence (NCAE) in Cybersecurity Symposium hosted by The College of Computing and Engineering

# Cybersecurity Graduate Research Symposium

**Nova Southeastern University (NSU)**
**Symposium hosted by The College of Computing and Engineering**
**October 11, 2023**

**Schedule**

**10:00-11:00** **Announcements and Breakfast**

**11:00-12:50** **Breakout Session A**

- **11:00-11:20** *A Comparison of Users' Personal Information Sharing Awareness, Habits, and Practices in Social Networking Sites and E-Learning Systems* by **Albert Ball, Ph.D. (In-Person)**
- **11:30-11:50** *Cyber Situational Awareness and Cyber Curiosity Taxonomy for Understanding Susceptibility of Social Engineering Attacks* by **Guillermo Perez, Ph.D. (In-Person)**
- **12:00-12:20** *Experimental Study to Assess the Role of Environment and Device Type on the Success of Social Engineering Attacks: The Case of Judgment Errors* by **Tommy Pollock, Ph.D. (In-Person)**
- **12:30-12:50** *Examining the Computer Security Behaviors of Telecommuters Working with Confidential Data through Leveraging the Factors from Fear Appeals Model (FAM)* by **Titus Fofung, Ph.D. (In-Person)**

**1:00-2:00** **Lunch Break**

**2:10-4:00** **Breakout Session B**

- **2:10-2:30** *Factors Motivating Employee Attitudes and Intentions to Share Knowledge in Homeland Security* by **Evette Maynard-Noel, Ph.D. (In-Person)**
- **2:40-3:00** *An Analysis of Differences in Behaviors and Practices of Security-Conscious Users and Regular Users on Mobile Devices by* **Stephen Mujeye, Ph.D. (In-Person)**
- **3:10-3:30** *The Game is Afoot: Using Tabletop Games to Understand Security and Privacy by* **Ann-Marie Horcher, Ph.D. (Zoom Link - https://nova.zoom.us/j/96392138378)**
- **3:40-4:00** *The Empirical Study of the Factors that Influence Threat Avoidance Behavior in Ransomware Security Incidents by* **Heriberto Acosta, Ph.D. (In-Person)**

**4:10-4:30** **Inaugural NSU College of Computing and Engineering Hall of Fame Induction - Loretta Neff**

**4:30-7:00** **Scotch Tasting Alumni Networking Reception – NSU Faculty Club**

***All times subject to change

Breakout Session A

**A Comparison of Users' Personal Information Sharing Awareness, Habits, and Practices in Social Networking Sites and E-Learning System**

Albert Ball, Ph.D.

Although reports of identity theft continue to be widely published, users continue to post an increasing amount of personal information online, especially within social networking sites (SNS) and e-learning systems (ELS). Research has suggested that many users lack awareness of the threats that risky online personal information sharing poses to their personal information. However, even among users who claim to be aware of security threats to their personal information, actual awareness of these security threats is often found to be lacking. Although attempts to raise users' awareness about the risks of sharing their personal information have become more common, it is unclear if users are unaware of the risks, or are simply unwilling or unable to protect themselves.

Research has also shown that users' habits may also have an influence on their practices. However, user behavior is complex, and the relationship between habit and practices is not clear. Habit theory has been validated across many disciplines, including psychology, genetics, and economics, with very limited attention in IS. Thus, the main goal of this study was to assess the influence of users' personal information sharing awareness (PISA) on their personal information sharing habits (PISH) and personal information sharing practices (PISP), as well as to compare the three constructs between SNS and ELS. Although habit has been studied significantly in other disciplines, a limited number of research studies have been conducted regarding IS usage and habit. Therefore, this study also investigated the influence of users' PISH on their PISP within the contexts of SNS and ELS. An empirical survey instrument was developed based on prior literature to collect and analyze data relevant to these three constructs. Path analysis was conducted on the data to determine the influence of users' PISA on their PISH and PISP, as well as the influence of users' PISH on their PISP. This study also utilized ANCOVA to determine if, and to what extent, any differences may exist between users' PISA, PISH, and PISP within SNS and ELS.

The survey was deployed to the student body and faculty members at a small private university in the Southeast United States; a total of 390 responses was received. Prior to final data analysis, pre-analysis data screening was performed to ensure the validity and accuracy of the collected data. Cronbach's Alpha was performed on PISA, PISH, and PISP, with all three constructs demonstrating high reliability. PISH was found to be the most significant factor evaluated in this study, as users' habits were determined to have the strongest influence on their PISP within the contexts of SNS and ELS.

The main contribution of this study was to advance the understanding of users' awareness of information security threats, their personal information sharing habits, and their personal information sharing practices. Information gained from this study may help organizations in the development of better approaches to the securing of users' personal information.

**Cyber Situational Awareness and Cyber Curiosity Taxonomy for Understanding Susceptibility of Social Engineering Attacks**
Guillermo Perez, Ph.D.

The maritime information system (IS) user has to be prepared to deal with a potential safety and environmental risk that can be caused by an unanticipated failure to a cyber system used onboard a vessel. A hacker leveraging a maritime IS user's Cyber Curiosity can lead to a successful cyber-attack by enticing a user to click on a malicious Web link sent through an email and/or posted on a social media website. At worst, a successful cyber-attack can impact the integrity of a ship's cyber systems potentially causing disruption or human harm. A lack of awareness of social engineering attacks can increase the susceptibility of a successful cyber-attack against any organization. A combination of limited cyber situational awareness (SA) of social engineering attacks used against IS users and the user's natural curiosity create significant threats to organizations.

The theoretical framework for this research study consists of four interrelated constructs and theories: social engineering, Cyber Curiosity, Cyber Situational Awareness, and activity theory. This study focused its investigation on two constructs, Cyber Situational Awareness and Cyber Curiosity. These constructs reflect user behavior and decision-making associated with being a victim of a social engineering cyber-attack. This study designed an interactive Web-based experiment to measure an IS user's Cyber Situational Awareness and Cyber Curiosity to further understand the relationship between these two constructs in the context of cyber risk to organizations. The quantitative and qualitative data analysis from the experiment consisting of 174 IS users (120 maritime & 54 shoreside) were used to empirically assess if there are any significant differences in the maritime IS user's level of Cyber SA, Cyber Curiosity, and position in the developed Cyber Risk taxonomy when controlled for demographic indicators.

To ensure validity and reliability of the proposed measures and the experimental procedures, a panel of nine subject matter experts (SMEs) reviewed the proposed measures/scores of Cyber SA and Cyber Curiosity. The SMEs' responses were incorporated into the proposed measures and scores including the Web-based experiment. Furthermore, a pilot test was conducted of the Web-based experiment to assess measures of Cyber SA and Cyber Curiosity. This research validated that the developed Cyber Risk taxonomy could be used to assess the susceptibility of an IS user being a victim of a social engineering attack. Identifying a possible link in how both Cyber SA and Cyber Curiosity can help predict the susceptibility of a social engineering attack can be beneficial to the IS research community. In addition, potentially reducing the likelihood of an IS user being a victim of a cyber-attack by identifying factors that improve Cyber SA can reduce risks to organizations. The discussions and implications for future research opportunities are provided to aid the maritime cybersecurity research and practice communities.

**Experimental Study to Assess the Role of Environment and Device Type on the Success of Social Engineering Attacks: The Case of Judgment Errors**
Tommy Pollock, Ph.D.

Phishing continues to be an invasive threat to computer and mobile device users. Cybercriminals continuously develop new phishing schemes using e-mail and malicious search engine links to gather the personal information of unsuspecting users. This information is used for financial gains through identity theft schemes or draining victims' financial accounts. Many users of varying demographic backgrounds fall victim to phishing schemes at one time or another. Users are often distracted and fail to process the phishing attempts fully, then unknowingly fall victim to the scam until much later. Users operating mobile phones and computers are likely to make judgment errors when making decisions in distracting environments due to cognitive overload. Distracted users cannot distinguish between legitimate and malicious emails or search engine results correctly. Mobile phone users can have a harder time distinguishing malicious content due to the smaller screen size and the limited security features in mobile phone applications.

The main goal of this research study was to design, develop, and validate experimental settings to empirically test if there are significant mean differences in users' judgment when: exposed to two types of simulated social engineering attacks (phishing & Potentially Malicious Search Engine Results (PMSER)), based on the interaction of the kind of environment (distracting vs. non-distracting) and type of device used (mobile vs. computer). This research used field experiments to test whether users are more likely to fall for phishing schemes in a distracting environment while using mobile phones or desktop/laptop computers. The second phase included a pilot test with 10 participants testing the Subject Matter Experts (SME) validated tasks and measures. The third phase included the delivery of the validated tasks and measures that were revised through the pilot testing phase with 68 participants.

The results of the first phase have SME validated two sets of experimental tasks and eight experimental protocols to assess the measures of users' judgment when exposed to two types of simulated social engineering attacks (phishing & PMSER) in two kinds of environments (distracting vs. non-distracting) and two types of devices (mobile phone vs. computer). The second phase results, the phishing mini-IQ test results, do not follow what was initially indicated in prior literature. Specifically, it was surprising to learn that the non-distracting environment results for the Phishing IQ tests were overall lower than those of distracting environment, which is counter to what was envisioned. These Phishing IQ test results may be assumed to be because, during the distracting environment, the participants were monitored over zoom to enable the distracting sound file. In contrast, in the non-distracting environment, they have marked the selections independently and may have rushed to identify the phishing samples.

In contrast, PMSER detection on a computer outperformed mobile devices. It is suspected that these results are more accurate as individuals' familiarity with PMSER is much lower. Their habituation to such messages is more deficient, causing them to pay closer attention and be more precise in their detections. A two-way Analysis of Variance (ANOVA) was conducted on the results. While it appears that some variations do exist, none of the comparisons were significant for Phishing IQ tests by environment ($F=3.714$, $p=0.061$) or device type ($F=0.380$, $p=0.541$), and PMSER IQ tests by environment ($F=1.383$, $p=0.247$) or device type ($F=0.228$, $p=0.636$). The results for the final phase showed there were no significant differences among both groups for Phishing and PMSER ($F=0.985$, $p=0.322$) and PMSER ($F=3.692$, $p=0.056$) using a two-way ANOVA. The two-way ANOVA results also showed significant differences among both groups for Phishing and PMSER vs. Device Type and Environment, Phishing ($F=3.685$, $p=0.013$), PMSER ($F=1.629$, $p=0.183$). A two-way ANOVA was evaluated for significant differences between groups. The results of the two-way ANOVA showed there were significant differences among both groups for Phishing and PMSER vs. Device Type and Environment. Phishing ($F=3.685$, $p=0.013$), PMSER ($F=1.629$, $p=0.183$). The p-values of the F-test for the Phishing IQ vs. Device Type and Environment were lower than the .05 level of significance. The two-way Analysis of Covariance (ANCOVA) results showed significant differences between Phishing vs. Environment and Device Type plus PMSER vs. Environment and Device Type. Specifically, the Education covariate for Table 32($F=3.930$, $p=0.048$), Table 33($F=3.951$, $p=0.048$), Table 34($F=10.429$, $p=0.001$), and Table 35($F=10.329$, $p=0.001$) was lower than the .05 level of significance.

**Examining the Computer Security Behaviors of Telecommuters Working with Confidential Data through Leveraging the Factors from Fear Appeals Model (FAM)**
Titus Fofung, Ph.D.

Computer users' security compliance behaviors can be better understood by devising an experimental study to examine how fear appeals might impact users' security behavior. Telecommuter security behavior has become relevant in information systems research with the growing number of individuals working from home. The home networks are usually not as secure as those in corporate settings. There is seldom a firewall setting, and the

software is not current. This study investigated how the home computer user's behavior can be modified, especially among telecommuters who work with sensitive data.

Breakout Session B

**Factors Motivating Employee Attitudes and Intentions to Share Knowledge in Homeland Security**

Evette Maynard-Noel, Ph.D.

The terrorist attacks of September 11, 2001, highlighted the inability of federal employees and officials to collaborate and share actionable knowledge-based information with the right people at the right time. However, much of the literature on knowledge sharing provided insight into knowledge sharing in private sector organizations and foreign public-sector organizations, instead of domestic public sectors or the United States federal government. While the importance of knowledge sharing for homeland security has been documented in the literature, there are no established frameworks that evaluate knowledge sharing motive and intentions in this context.

The main goal of this research was to understand what motivates employee attitudes and intentions to share knowledge, by empirically assessing a model, testing the impact of the factors of expected rewards, expected contributions, expected associations, trust, and information technology (IT) type and usage on employee attitudes and intentions toward knowledge sharing in homeland security.

The technology acceptance model and the theory of reasoned action served as the theoretical framework to understand motivation factors that affect employee attitudes, intentions, and their influence on knowledge sharing behaviors, as well as the technology used in sharing knowledge.

Data were collected from employees and affiliates of the United States Department of Homeland Security (N = 271), using a Web-based survey. The effects of expected rewards, expected contributions, expected associations, trust, and IT type usage were studied using regression analyses. The statistical results revealed that expected contributions and expected associations were positively related to attitudes to share knowledge, but expected rewards were not significantly related to attitudes to share knowledge. Results also revealed that attitudes to share knowledge was positively related to intentions to share knowledge, but trust did not significantly moderate this relationship.

Finally, the results revealed that intentions to share knowledge was positively related to knowledge sharing, and IT-type usage positively moderated this relationship. The research model showed significant results to support five of the seven hypotheses proposed and revealed key findings on factors that influence employee attitudes and intentions to share knowledge in homeland security. This research advances prior findings and contributes to knowledge sharing research, practice, and overall literature regarding knowledge sharing, individual behaviors, attitudes, and intentions to share knowledge, technology acceptance, and usage. This contribution to the body of knowledge provides researchers, policymakers, and decision-makers with foundations for improving collaboration through information and knowledge sharing across traditional and nontraditional organizational boundaries.

**An Analysis of Differences in Behaviors and Practices of Security-Conscious Users and Regular Users on Mobile Device**
Stephen Mujeye, Ph.D.

Mobile devices are widespread worldwide; individuals increasingly use them to check emails, online banking, social media, etc. Previous studies have shown, however, that mobile devices have specific weaknesses and vulnerabilities to security. Security attacks for mobile users have also been on the increase. This study investigated the differences in security-conscious (group A) and regular (group B) users' behaviors and practices on mobile devices. A survey was used to investigate the differences in behaviors and practices of security-conscious users (group A) and regular users (group B) on mobile devices. Each group had 50 participants, for a total of 100. The analysis revealed that differences are present in the behaviors and practices of security-conscious users and regular users. The results indicated that security-conscious users engage in behaviors and practices that are more secure on mobile devices when compared with regular users. The results will help recommend the best behaviors and practices for mobile device users, increasing mobile device security. The results will help society to be more aware of security behaviors and practices on mobile devices.

**The Game is Afoot: Using Tabletop Games to Understand Security and Privacy**
Ann-Marie Horcher, Ph.D.

In spite of a growing addiction to screens and video games, Tabletop Role-playing Games (TTRPG) and card games are experiencing a golden age of popularity. Though Capture the Flag (CTF) games on online platforms are a mainstay of cybersecurity education, the use of tabletop games is not. This research examines how interaction with TTRPG and also the game design process can yield a better understanding of security and privacy concepts. Furthermore, inclusion of under- represented populations into game design can yield game content more inclusive to that population.

**The Empirical Study of the Factors that Influence Threat Avoidance Behavior in Ransomware Security Incidents**
Heriberto Acosta, Ph.D.

Ransomware is a significant threat to computer users, including college students. This study examines factors influencing threat avoidance among students facing ransomware incidents. Data from 174 US students reveals a positive link between avoidance motivation and threat avoidance behavior. Subjective norm was found to affect knowledge sharing attitude but not response efficacy. This research sheds light on students' readiness to combat ransomware threats.

**Inaugural NSU College of Computing and Engineering Hall of Fame Induction - Loretta Neff**

Loretta Neff has been a role model for women in technology for over 40 years. Loretta, who is originally from Pennsylvania, attended North Miami High School and graduated in 1956. She then attended Barry College and earned an associate degree in accounting and business in 1958. During this time, she started in finance working at Ford Motor Credit before moving to California as chief accountant at United Recording Corp. Loretta chose to join the group that worked on their first computer system. After some time there, she returned to Miami and took evening classes in programming which was basic assembler and machine language. She went on to work for Burroughs Corporation for 30 years and was assigned various work including programming and installations. Loretta earned her bachelors and masters at Nova Southeastern University and has been an active alumni supporting women in technology. Loretta went on to work for Ameriprise Financial for several years as a financial advisor. She eventually returned to Burroughs and was assigned to be the manager of human resource software until she retired in 2006. Loretta now serves on the foundation board of John Knox Village.