4th Annual College of Computing, AI, and Cybersecurity Research Symposium
Nova Southeastern University (NSU)
October 28, 2026

Schedule

11:00-11:30 **Welcome and Opening Remarks by Dr. Greg Simco | Refreshments**

11:35-12:55 **Breakout Session A**

11:35-11:55 *Governance, Ethics, and Institutional Preparedness for Emerging Intelligent Systems by* **George Antoniou**

12:05-12:25 *Privacy and Security Matters related to College Students App usage by* **Richard Maiti**

12:35-12:55 *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**

1:00-2:00 **Lunch and Networking**

2:10-4:30 **Breakout Session B**

2:10-2:30 *Beyond CVSS: Design and Evaluation of an Explainable Vulnerability Prioritization Decision Framework (VPDF) by* **Stephen Mujeye**

2:40-3:00 *Cybersecurity, Artificial Intelligence, and the Protection of Space Assets by* **Heriberto Acosta-Maestre**

3:10-3:30 *Research Recipes: Making Cybersecurity Labs out of Research Studies by* **Ann-Marie Horcher (Virtual)**

3:40-4:00 *Comparative Evaluation of Data Augmentation Strategies for Rare-Class Intrusion Detection: Assessing Conditional Generative Adversarial Networks Across Benchmark Datasets and Classifiers by* **Brogan O'Connor**

4:10-4:30 *A Universal Cybersecurity Competency Framework for Organizational Users by* **Patricia Baker**

4:30-7:00 **Scotch Tasting Reception & Computing Hall of Fame Induction Honoring Alexander Raymond Corris | NSU Shark Club**

4th Annual College of Computing, AI, and Cybersecurity Research Symposium
Nova Southeastern University (NSU)
October 28, 2026

Welcome to the 4th Annual College of Computing, AI, and Cybersecurity Research Symposium! Over the years, the Symposium has provided an opportunity to recognize individuals who have made meaningful contributions to the field of computing and technology. In 2023, we inducted Loretta Neff into NSU's Computing Hall of Fame, followed by John Machado in 2024 and Victoria Ranger Nunez in 2025. This year, we are proud to continue that tradition by inducting Dr. Alexander Raymond Corris, Senior Director of Football Systems for the Miami Dolphins, into NSU's Computing Hall of Fame.

Nova Southeastern University has been designated as a National Center of Academic Excellence in Cybersecurity (NCAE-C) Cyber Defense (CD) and Cyber Research (R) through the academic year 2028. This new designation complements our re-designation as a National Center of Academic Excellence in Cybersecurity in 2021.

Breakout Session A

Governance, Ethics, and Institutional Preparedness for Emerging Intelligent Systems.
George Antoniou

Artificial intelligence is rapidly transforming institutions, yet many organizations remain unprepared to address governance, ethical, cybersecurity, and operational challenges associated with emerging intelligent systems. This research proposes an AI Readiness Capability Maturity perspective informed by cybersecurity governance, institutional resilience, and AI risk management frameworks, including NIST and European Union initiatives. Drawing from international collaboration and Fulbright research activities, the study examines how institutions can evaluate readiness across governance, ethics, workforce preparedness, cybersecurity, and operational integration.

Privacy and Security Matters related to College Students App usage
Richard Maiti

As mobile applications become deeply integrated into the academic and social infrastructure of higher education, college students increasingly expose vast amounts of personal data to diverse third-party ecosystems. This paper extends prior research on mobile devices and social media vulnerabilities by critically examining the unique privacy and security paradigms surrounding college students' app usage. While mobile applications facilitate seamless campus integration, communication, and learning management, they also introduce heightened risks of data harvesting, location tracking, and unauthorized access to credentials. This study investigates student risk awareness, common app permissions conceded during daily use, and the potential exploitation of these vulnerabilities by malicious actors. By analyzing user behavior alongside data-sharing mechanisms, we expose a critical gap between student privacy concerns and actual permission-granting habits. Ultimately, this paper proposes a multi-layered mitigation framework—combining enhanced institutional mobile policies, user-centric privacy controls, and targeted security awareness education—to safeguard sensitive student data within an increasingly interconnected academic ecosystem.

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

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.

Breakout Session B

Beyond CVSS: Design and Evaluation of an Explainable Vulnerability Prioritization Decision Framework (VPDF).
Stephen Mujeye

Organizations face more software vulnerabilities than security teams can remediate, while conventional prioritization methods such as CVSS may not adequately reflect exploitation or organizational risk. This study proposes an explainable Vulnerability Prioritization Decision Framework (VPDF) using Design Science Research. VPDF integrates CVSS, EPSS, KEV status, machine-learning predictions, and organizational context to support remediation decisions. The framework will be evaluated through technical validation, expert refinement, a quasi-experiment comparing VPDF-assisted and CVSS-based triage, and interviews. The study examines whether explainable decision support improves decision quality, efficiency, consistency, and analyst trust.

Cybersecurity, Artificial Intelligence, and the Protection of Space Assets
Heriberto Acosta-Maestre

The security of space assets depends on the digital infrastructure connecting satellites, ground systems, and users. A cyber intrusion on Earth can compromise a space mission without physically damaging anything in orbit. These dependencies have direct implications for military operations, critical infrastructure, and the commercial services that support them.

This presentation examines how cybersecurity and artificial intelligence shape the protection and use of space assets. It considers vulnerabilities across the systems that deliver space-based services, focusing on unauthorized access, data manipulation, and disruption of mission functions. The discussion then addresses AI applications in anomaly detection, satellite-data analysis, and mission planning. Attention is given to the security of the AI systems themselves, including their exposure

to manipulated inputs and the consequences of relying on inaccurate outputs in operational decisions.

Using operational examples relevant to the Western Hemisphere, the presentation connects these issues to defense planning and dependence on commercial space providers. Its central argument is that cybersecurity and responsible AI use belong within mission planning, procurement, and operational oversight. The discussion closes with practical priorities for decision-makers, including maintaining essential services during a disruption, establishing responsibility across government and industry, and preserving human judgment in AI-supported operations.

Research Recipes: Making Cybersecurity Labs out of Research Studies
Ann-Marie Horcher

The research community has been creating and solving security usability challenges for two decades. Several conferences welcome replication of previous studies both to validate the original interpretation, and to apply the concepts to new and similar technologies. These studies also have a wider application to the cybersecurity education community. Security usability has been identified as a key risk in OWASP and other threat predictors. The materials to teach these concepts lag far behind more technical concepts such as remote machines and tool simulations. In particular, rules for creating strong passwords evolve regularly, and the research that sets those rules may need re-validation in the wake of current technologies. This research replicates a study from 2015 that examined the user acceptance and ability to learn long passwords. The original instruments were re-created using current technology and the original conclusions re-examined based on current risks and password norms. The objective is to create relevant hands-on exercises (labs) in a cybersecurity curriculum to teach seminal and once radical concepts in security usability.

Comparative Evaluation of Data Augmentation Strategies for Rare-Class Intrusion Detection: Assessing Conditional Generative Adversarial Networks Across Benchmark Datasets and Classifiers
Brogan O'Connor

Intrusion Detection Systems (IDS) are widely used to identify malicious network activity, unauthorized access, and anomalous system behavior. Although machine learning and deep learning classifiers often achieve strong aggregate performance on IDS benchmark datasets, rare attack detection remains difficult because of severe class imbalance. Minority attack categories may contain very few training observations, which can bias classifiers toward normal traffic and more frequent attack classes. This problem is especially important because rare attacks may represent high-impact security events even when they occur infrequently.

This quantitative experimental study evaluated whether conditional generative adversarial network (cGAN) augmentation improved rare attack detection in supervised IDS classification. The study compared cGAN augmentation with four alternative training conditions: no augmentation, Synthetic Minority Oversampling Technique (SMOTE), Adaptive Synthetic Sampling (ADASYN), and standard generative adversarial network (GAN) augmentation. Experiments were

conducted across three IDS benchmark datasets: NSL-KDD, UNSW-NB15, and CICIDS2017. Five classifier families were evaluated for each dataset and augmentation condition: Random Forest, Support Vector Machine (SVM), XGBoost, Convolutional Neural Network (CNN), and Long Short-Term Memory (LSTM). Performance was measured using accuracy, precision, recall, F1-score, false positive rate, and area under the receiver operating characteristic curve (AUC-ROC), with emphasis on macro recall, macro F1-score, and minority-class performance.

Results showed that cGAN augmentation was competitive in selected settings but did not outperform the best overall method on any dataset. On CICIDS2017, the strongest overall result was produced by baseline XGBoost, with a macro F1-score of 0.9181. On NSL-KDD, the strongest overall result was produced by SMOTE with SVM, with a macro F1-score of 0.6125. On UNSW-NB15, the strongest overall result was produced by baseline XGBoost, with a macro F1-score of 0.5186. The best cGAN models closely matched the strongest results on CICIDS2017 and UNSW-NB15 but trailed more substantially on NSL-KDD.

The findings indicate that cGAN augmentation should not be assumed to outperform traditional resampling or strong unaugmented classifiers in imbalanced IDS classification. Instead, its usefulness depends on the dataset, target class, classifier, and quality of the generated synthetic observations. This study contributes a reproducible, multi-dataset, multi-classifier evaluation of conditional generative augmentation for minority-class IDS detection and reinforces the importance of evaluating rare attack performance with macro-level and per-class metrics rather than accuracy alone.

A Universal Cybersecurity Competency Framework for Organizational Users
Patricia Baker

The global reliance on the Internet to facilitate organizational operations necessitates further investments in organizational information security. Such investments hold the potential for protecting information assets from cybercriminals. To assist organizations with their information security, The National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework (NCWF) was created. The framework referenced the cybersecurity work, knowledge, and skills required to competently complete the tasks that strengthen their information security. Organizational users' limited cybersecurity competency contributes to the financial and information losses suffered by organizations year after year. While most organizational users may be able to respond positively to a cybersecurity threat, without a measure of their cybersecurity competency they represent a cybersecurity threat to organizations.

The main goal of this research study was to develop a universal Cybersecurity Competency Framework (CCF) to determine the demonstrated cybersecurity Knowledge, Skills, and Tasks (KSTs) through the NCWF (NICE, 2017) as well as identify the cybersecurity competency of organizational users. Limited attention has been given in cybersecurity research to determine organizational users' cybersecurity competency. An expert panel of cybersecurity professionals known as Subject Matter Experts (SMEs) validated the cybersecurity KSTs necessary for the universal CCF. The research study utilized the explanatory sequential mixed-method approach to develop the universal CCF.

This research study included a developmental approach combining quantitative and qualitative data collection in three research phases. In Phase 1, 42 SMEs identified the KSTs needed for the universal CCF. The results of the validated data from Phase 1 were inputted to construct the Phase 2 semi-structured interview. In Phase 2, qualitative data were gathered from 12 SMEs. The integration of the quantitative and qualitative data validated the KSTs. In Phase 3, 20 SMEs validated the KST weights and identified the threshold level. Phase 3 concluded with the SMEs' aggregation of the KST weights into the universal CCF index.

The weights assigned by the SMEs in Phase 3 showed that they considered knowledge as the most important competency, followed by Skills, then Tasks. The qualitative results revealed that training is needed for cybersecurity tasks. Phase 3 data collection and analysis continued with the aggregation of the validated weights into a single universal CCF index score. The SMEs determined that 72% was the threshold level.

The findings of this research study significantly contribute to the body of knowledge on information systems and have implications for practitioners and academic researchers. It appears this is the only research study to develop a universal CCF to assess the organizational user's competency and create a threshold level. The findings also offer further insights into what organizations need to provide cybersecurity training to their organizational users to enable them to competently mitigate cyber-attacks.