1. Record Nr. UNINA9911074253203321

Titolo	Suppression of liquor traffic among Indians. December 10 (calendar day, December 13), 1924. -- Ordered to be printed
Pubbl/distr/stampa	Washington, DC : , : [publisher not identified], , 1924
Descrizione fisica	1 online resource (2 pages)
Collana	Senate report / 68th Congress, 2nd session. Senate ; ; no. 805 [United States congressional serial set] ; ; [serial set no. 8388]
Altri autori (Persone)	HarreldJohn W (Republican (OK))
Soggetti	Indian reservations Legislative amendments Liquor laws Searches and seizures Warrants (Law) Legislative materials.
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Batch processed record: Metadata reviewed, not verified. Some fields updated by batch processes. FDLP item number not assigned. Electronic resource.

2. Record Nr. UNINA9910865237803321

Autore	Moallem Abbas
Titolo	HCI for Cybersecurity, Privacy and Trust : 6th International Conference, HCI-CPT 2024, Held as Part of the 26th HCI International Conference, HCII 2024, Washington, DC, USA, June 29–July 4, 2024, Proceedings, Part II / / edited by Abbas Moallem
Pubbl/distr/stampa	Cham : , : Springer Nature Switzerland : , : Imprint : Springer, , 2024
ISBN	9783031613821
Edizione	[1st ed. 2024.]
Descrizione fisica	1 online resource (267 pages)
Collana	Lecture Notes in Computer Science, , 1611-3349 ; ; 14729
Disciplina	005.437 004.019
Soggetti	User interfaces (Computer systems) Human-computer interaction Coding theory Information theory Computers - Law and legislation Information technology - Law and legislation Computer networks Electronic commerce Software engineering User Interfaces and Human Computer Interaction Coding and Information Theory Legal Aspects of Computing Computer Communication Networks e-Commerce and e-Business Software Engineering
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di contenuto	Intro -- Foreword -- HCI International 2024 Thematic Areas and Affiliated Conferences -- List of Conference Proceedings Volumes Appearing Before the Conference -- Preface -- 6th International Conference on HCI for Cybersecurity, Privacy and Trust (HCI-CPT 2024)

-- HCI International 2025 Conference -- Contents - Part II -- Contents - Part I -- Cybersecurity Education and Training -- Decoding the Human Element in APT Attacks: Unveiling Attention Diversion Techniques in Cyber-Physical System Security -- 1 Introduction -- 2 Background and Related Work -- 3 Methodology and Concept -- 3.1 Definition of Attention Diversion in Cybersecurity -- 3.2 Techniques of Attention Diversion -- 3.3 Conceptual Framework -- 4 Case Study -- 4.1 Digital Station (DS) Enclave Testbed -- 4.2 Constructing the Cover Story -- 4.3 Summary of the Covering Story -- 4.4 Attack Steps -- 5 Conclusion and Future Work -- References -- Competencies Required for the Offensive Cyber Operations Planners -- 1 Introduction -- 2 Methods -- 2.1 Review Procedure -- 2.2 Literature Collection Methodology -- 3 Results -- 3.1 Training Plan -- 3.2 Knowledge -- 3.3 Skillset -- 3.4 Abilities -- 3.5 Experience -- 4 Discussion -- 5 Limitations and Future Work -- 6 Conclusions -- References -- Unraveling the Real-World Impacts of Cyber Incidents on Individuals -- 1 Introduction -- 2 Methods -- 2.1 Identifying Areas of Cyber Incidents -- 2.2 Interview Design -- 2.3 Participant Recruitment -- 2.4 Data Collection -- 2.5 Interview Data Analysis -- 3 Results -- 3.1 Survey -- 3.2 Interviews -- 3.3 Themes -- 4 Discussion -- 5 Conclusion -- References -- Experiential Learning Through Immersive XR: Cybersecurity Education for Critical Infrastructures -- 1 Introduction -- 2 Literature Review -- 2.1 XR-Enabled Immersive Training Experiences -- 2.2 Cybersecurity Training and Education Challenges.
2.3 Innovations in Cybersecurity Training Platforms -- 3 The Proposed Use-Case: An XR-Enabled Waste Water Treatment Educational Testbed -- 4 System Overview -- 5 The Main System Actors -- 5.1 Physical AI Agent -- 5.2 Conversational AI Agent -- 5.3 The XR Environment -- 6 Qualitative Evaluation -- 6.1 XR Environment -- 6.2 Physical AI Agent -- 7 Conclusions and Future Work -- References -- Revolutionizing Social Engineering Awareness Raising, Education and Training: Generative AI-Powered Investigations in the Maritime Domain -- 1 Introduction -- 2 Relevant Work -- 3 Methodology -- 4 Exploration Aspects -- 4.1 Social Engineering Attacks -- 4.2 Business Environment -- 5 Analysis of Generative AI Responses -- 6 Discussion -- 7 Conclusions -- References -- Training and Security Awareness Under the Lens of Practitioners: A DevSecOps Perspective Towards Risk Management -- 1 Introduction -- 2 Background -- 2.1 DevSecOps and Risk Management -- 2.2 Training and Security Awareness -- 3 Research Approach -- 3.1 Survey Design -- 3.2 Data Collection -- 3.3 Data Analysis -- 4 Results and Discussion -- 4.1 Demographic Information -- 4.2 Training and Security Awareness (RQ1) -- 4.3 DevOps and Risk Management Practices (RQ2) -- 4.4 Threats to Validity -- 5 Conclusions -- References -- Expert Perspectives on Information Security Awareness Programs in Medical Care Institutions in Germany -- 1 Introduction -- 2 Background -- 2.1 Information Security in Healthcare Facilities in Germany -- 2.2 Information Security Awareness in the Medical Care Sector -- 2.3 Contributions -- 3 Methodology -- 3.1 Ethical Concerns -- 3.2 Study Procedure and Analysis -- 3.3 Participants -- 3.4 Limitations -- 4 Findings -- 4.1 The Human Factor and the ``Human Firewall'' -- 4.2 Goals, Target Groups, and Implementation of ISA -- 4.3 Development and Evaluation of ISA Materials.
4.4 Structural Problems of Information Security in Medical Care -- 5 Discussion -- 5.1 Summary -- 5.2 Implications -- 6 Conclusions -- References -- Threat Assessment and Protection -- Whisper+AASIST for DeepFake Audio Detection -- 1 Introduction -- 1.1 Motivation -- 1.2 Research Question -- 2 Related Works -- 2.1 Overview -- 2.2 State

of the Art -- 2.3 The AASIST Architecture -- 2.4 Whisper -- 3 Methods and Data -- 3.1 Methods -- 3.2 Data -- 3.3 Implementation Details -- 4 Results -- 5 Discussion -- 6 Conclusion -- References -- Paralyzed or Compromised: A Case Study of Decisions in Cyber-Physical Systems -- 1 Introduction -- 2 Related Work and Background -- 2.1 CPSs -- 2.2 Human Operators in CPSs -- 2.3 Situation Awareness -- 2.4 The Sunburst Attack -- 3 Method -- 4 Findings -- 4.1 The Sunburst Case from the Actors' Perspective -- 4.2 Themes Identified in the Analysis -- 4.3 Logic Model of Decision Making -- 5 Discussion -- 6 Conclusion -- References -- Cognitive Digital Twins for Improving Security in IT-OT Enabled Healthcare Applications -- 1 Introduction -- 1.1 Overview -- 1.2 Our Contributions -- 1.3 Structure of the Paper -- 2 Related Work -- 3 Proposed Framework -- 4 Use Cases and Scenarios -- 4.1 Personalized Patient Care and Treatment -- 4.2 Remote Patient Monitoring -- 4.3 Assistive and Social Robots in Care -- 4.4 Enhancing Resilience in Healthcare Technologies -- 5 Conclusions and Future Work Directions -- References -- Viz4NetSec: Visualizing Dynamic Network Security Configurations of Everyday Interconnected Objects in Home Networks -- 1 Introduction -- 1.1 First Goal: Visualization for Simple Smart Home Tasks -- 1.2 Second Goal: Dynamicity of the Exercised Control -- 2 Related Work -- 2.1 Network Security Configuration -- 2.2 Network Security Visualization -- 2.3 Home User Scenarios.
3 Viz4NetSec: A Network Visualization for Improving Home Network Security Through Dynamic Interaction -- 3.1 Technical Prototype Using Open-Source Components -- 3.2 Features of Viz4NetSec -- 4 Discussion and Future Work -- 4.1 Algorithmic Efficiency -- 4.2 Usability and Learnability -- 4.3 Component Interoperability -- 4.4 Cognitive Workload and Task Performance -- 4.5 Feature Set Utility -- 5 Conclusion -- References -- Authentication Method Using Opening Gestures -- 1 Introduction -- 2 Related Research -- 2.1 Authentication Methods Leveraging Capacitive Sensing -- 2.2 Authentication Methods Leveraging Pressure Sensing -- 2.3 Authentication Methods Leveraging IMU Sensing -- 2.4 Authentication Methods Leveraging Opening Gesture -- 3 Exploring the Design Space of Opening Gestures -- 3.1 Participants -- 3.2 Hardware -- 3.3 Procedure -- 3.4 Results -- 3.5 Feature Visualization -- 3.6 Machine Learning -- 4 Experiment: Shoulder Hacking -- 4.1 Participants -- 4.2 Procedure -- 4.3 Results -- 4.4 Feature Visualization -- 4.5 Machine Learning -- 5 Discussion and Future Work -- 6 Conclusion -- References -- Investigating University QR Code Interactions -- 1 QR Codes: Human-Centered Cybersecurity -- 2 End User Vulnerability and Risk Mitigation -- 3 Studying University QR Interactions -- 3.1 Addressing Ethical Concerns -- 3.2 Procedure -- 3.3 Apparatus and Stimuli -- 3.4 Participants -- 4 Results -- 4.1 Viewing Time -- 4.2 Engagement by Flyer Type -- 4.3 University Logo Survey Responses -- 5 Discussion -- References -- Exploring ICS/SCADA Network Vulnerabilities -- 1 Introduction -- 2 Literature Review -- 3 Methodology -- 3.1 CIS Critical Security Controls (CIS Controls) -- 3.2 Factor Analysis of Information Risk (FAIR) -- 4 Conducting the Research -- 4.1 Asset Identification and Vulnerability Assessment -- 4.2 Risk Assessment.
4.3 Feasibility Study and Effectiveness Evaluation -- 5 Findings and Results -- 5.1 Asset Identification -- 5.2 Vulnerability Assessment -- 5.3 Risk Assessment -- 5.4 Mitigation Measures -- 6 Conclusion -- 6.1 Summary of Findings -- 6.2 Limitations -- References -- Electrical Muscle Stimulation System for Automatic Reproduction of Secret Information Without Exposing Biometric Data -- 1 Introduction -- 2 Related Work -- 2.1 Password-Less Authentication -- 2.2 EMS -- 3

Human Parameterized Locality Sensitive Hash -- 3.1 Issues with the Current Biometric System -- 3.2 Approach to Solving the Problem: HPLSH -- 3.3 EMS-Type HPLSH -- 4 Password-Less Authentication Using HPLSH -- 4.1 Registration Procedure -- 4.2 Authentication Procedure -- 4.3 Management of Secret Information -- 5 Preliminary User Experiments -- 5.1 Identification of Electrical Stimulation "s" -- 5.2 User Authentication -- 6 Discussion -- 6.1 Challenges of the Proposed Method -- 6.2 Application of the Proposed Method -- 7 Conclusion -- References -- Author Index.

Sommario/riassunto

This proceedings, HCI-CPT 2024, constitutes the refereed proceedings of the 6th International Conference on Cybersecurity, Privacy and Trust, held as Part of the 26th International Conference, HCI International 2024, which took place from June 29 - July 4, 2024 in Washington DC, USA. Two volumes of the HCII 2024 proceedings are dedicated to this year’s edition of the HCI-CPT Conference. The first focuses on topics related to Cyber Hygiene, User Behavior and Security Awareness, and User Privacy and Security Acceptance. The second focuses on topics related to Cybersecurity Education and Training, and Threat Assessment and Protection.