Faculty	Management and Social Sciences
Department	Sociology
Course Title	**Cyber Crimes**
Year of Study	4
Course Code	CSS 414
Credit Hours	2
Contact Hours	30
Mode of Delivery	Classroom Lectures

Mode of Assessment	**Weight%**
Continuous Assessment	30%
Final Examination	70%
Total	100%

Course Lecture/Instructor	MR A. A. AJIBADE
Course Description	An examination of crimes involving the use of computers; Topics include federal and state laws and investigative and preventive methods used to secure computers. Case studies emphasize security.
Course Objectives	At the end of this course students should be able to examine crimes involving the use of computers; Topics include federal and state laws and investigative and preventive methods used to secure computers. Case studies emphasize security.
Learning Outcomes	At the end of this course students will be able to examine crimes involving the use of computers; Topics include federal and state laws and investigative and preventive methods used to secure computers. Case studies emphasize security. groups; legal policies about trade, migration and rights of refugees; legal policy issues in Nigeria.
Teaching and Learning	The class will meet for two hours each week. Class time will be used for a combination of lectures and practical sessions
Detailed Course Content	examine crimes involving the use of computers; Topics include federal and state laws and investigative and preventive methods used to secure computers. Case studies emphasize security.

Course Content Sequencing

Weeks	**Detailed Course Outline**	**Allocated Time**
Week 1	Introduction to Cybercrime Definition and scope of cybercrimes Historical context and evolution of cybercrime Key terminology and concepts in cybercrime	2 hours
Week 2	Federal Cybercrime Laws Overview of key federal laws (e.g., Computer Fraud and Abuse Act) Jurisdiction and federal agencies involved in cybercrime enforcement Case studies illustrating federal cybercrime prosecutions	2 hours
Week 3	Cybercrime Laws Examination of state-level cybercrime legislation	2 hours

	Variations in cybercrime laws across different states Comparative analysis of federal vs. state cybercrime laws	
Week 4	Investigative Techniques I Digital forensics: Collecting and preserving electronic evidence Tools and technologies for cybercrime investigation Chain of custody and legal admissibility of digital evidence	2 hours
Week 5	Investigative Techniques II Profiling cybercriminals and understanding their motives Analyzing attack vectors and tactics Ethical considerations in cybercrime investigations	2 hours
Week 6	Preventive Measures Overview of cybersecurity best practices Risk assessment and threat modeling Security policies and incident response planning	2 hours
Week 7	Case Study 1 - Data Breaches In-depth analysis of high-profile data breach cases Identifying vulnerabilities and lessons learned Legal consequences for organizations involved	2 hours
Week 8	Case Study 2 - Identity Theft Exploring identity theft cases and their impact on victims Methods used by cybercriminals to steal identities Legal and ethical aspects of identity theft prevention	2 hours
Week 9	Case Study 3 - Financial Cybercrimes Examining financial fraud cases and their economic implications Techniques used in financial cybercrimes (e.g., phishing, ransomware) Strategies for financial institutions to combat cybercrime	2 hours
Week 10	International Cybercrime and Law Enforcement Cooperation Challenges of cross-border cybercrime investigations International treaties and agreements related to cybercrime Examples of successful international cybercrime collaborations	2 hours
Week 11	Emerging Trends and Future of Cybercrime Discussion of current and emerging cyber threats Technologies shaping the future of cybercrime Preparing for the evolving landscape of cybercrime prevention and investigation	2 hours
Week 14	Examination	
RECOMMENDED MATERIALS **Textbooks:**		

Casey, Eoghan. (2018). "Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet." Academic Press.

Schell, Bernadette H., & Martin, Clemens. (2020). "Cybercrime: The Transformation of Crime in the Information Age." Wiley.

Goodrich, Michael T., & Tamassia, Roberto. (2014). "Introduction to Computer Security." Pearson.

Journal Articles:

Yar, Majid. (2013). "The Novelty of 'Cyber Terrorism': Research Problems and Prospects." Studies in Conflict & Terrorism, 36(11), 943-962.

Taylor, Robert W., & Fritsch, Eric J. (2015). "Digital Crime and Digital Terrorism." Pearson.

Government Publications:

United States Department of Justice. (2021). "Computer Crime & Intellectual Property Section (CCIPS)." https://www.justice.gov/criminal-ccips

Federal Bureau of Investigation (FBI). (2021). "Cyber Crime." https://www.fbi.gov/investigate/cyber

Online Resources:

Cybersecurity & Infrastructure Security Agency (CISA). (2021). "Cybersecurity Resources." https://www.cisa.gov/cybersecurity-resources

Krebs on Security. (2021). "In-Depth Security News and Investigation." https://krebsonsecurity.com/

Case Studies:

Various news articles and reports on cybercrime incidents and investigations. These can be found on reputable news websites and official law enforcement sources.
Academic Journals:

Access academic journals such as the "Journal of Cybersecurity" and "Digital Investigation" for scholarly articles related to cybercrime and computer security.