# San José State University
# Department of Justice Studies
# JS 161: Introduction to Cybercrime
# Summer 2022

## Course and Contact Information

| | |
|---|---|
| **Instructor:** | Dr. Bryce Westlake |
| **Office Location:** | Health Building 210B |
| **Email:** | Bryce.Westlake@sjsu.edu |
| **Office Hours:** | Monday & Thursday 10:00am to 12:00pm |
| **Prerequisites:** | Any 100w |

## Course Format

### Technology Intensive, Hybrid, and Online Courses

I will utilize the Canvas Learning Management System as a means for distributing course materials such as syllabus, handouts, lecture slides, assignment instructions, and communications about changes to the course. You are responsible for regularly checking with the messaging system through MySJSU to learn of updates.

### Catalog Description

Introduces students to the growing legal, technical, and social issues surrounding crimes committed in cyberspace or assisted by computers. Discusses the nature of cybercrime from an international perspective and how the borderless nature of cybercrime impacts regulation and enforcement.

### Course Description

This course explores how an interconnected world has modified how existing criminal activity is conducted and how new criminal opportunities have been created. Students will examine the history and complex nature of computer-related crime and how societies have attempted to respond. Students will discuss the different types of cybercriminals, including motives, rationale, and methods of attack. We will also evaluate various legal and regulatory issues in cyberspace, including surveillance, sting operations, current and proposed legislation, user-reporting initiatives, identity filtering/blocking technologies, vigilante movements, individual rights, and international law enforcement cooperation.

### Course Goals

The Department of Justice Studies is committed to scholarly excellence. Therefore, the Department promotes academic, critical, and creative engagement with language (i.e., reading and writing) throughout its curriculum. A sustained and intensive exploration of language prepares students to think critically and to act meaningfully in interrelated areas of their lives–personal, professional, economic, social, political, ethical, and cultural. Graduates of the Department of Justice Studies leave San José State University prepared to enter a range of careers and for advanced study in a variety of fields; they are prepared to more effectively identify and ameliorate injustice in their personal, professional and civic lives. Indeed, the impact of literacy is evident not only within the span of a specific course, semester, or academic program but also over the span of a lifetime.

## Course Learning Outcomes (CLO)

Upon successful completion of this course, students will be able to:

> (CLO 1) distinguish between the different types of cybercrimes, including who/what they target, how/where they are conducted, and why they persist.

> (CLO 2) describe the impacts of the Internet on the opportunities created for committing traditional crimes (e.g., bullying) and new crimes (e.g., phishing).

> (CLO 3) identify the challenges faced nationally and internationally at combating cybercrime and the steps taking by organizations to address these challenges.

> (CLO 4) use what they have learned to increase their own security and privacy when online.

> (CLO 5) apply what they have learned to cybercrime-related current events.

## Required Readings

**Textbook:** None.
**Articles:** supplied electronically via Canvas.

## Library Liaison

Megwalu, Anamika (anamika.megwalu@sjsu.edu) (408) 808.2089
*https://libguides.sjsu.edu/cybersecurity*

## Course Requirements and Assignments

*Online Discussion (20%):* There will be two discussion questions each week, examining specific elements and key issues or current events related to that lecture's overall topic. Students will be expected to provide their viewpoint and critically discuss the implications of the issue or event to our understanding of cybercrime and how it is addressed by societies. This assignment will specifically address CLO's 1, 2, 3, 4, & 5.

*Paper #1 –Tell Me a Story (20%):* The purpose of this assignment is to provide students with practical experience to explore the concept of personal privacy, or lack thereof, on the Internet. Students will write a short six to eight-page paper (excluding title page and references) on their investigation of two topics. First, students will input their name into a search engine, with minimal other identifying information, and describe whether the data returned was about them, and how they felt about that information being readily accessible. They will describe the age (i.e., how old), personal nature (e.g., address, phone number, banking information), and online profile (e.g., your likes/dislikes, purchases, hobbies) it presented about them. Second, students will use any cyber methods they can devise to find information on the course instructor. Students will be required to record the steps they took (e.g., search terms) to acquire the information and what information they obtained, including where it was found. Students will then describe this process and reflect on the steps others may take to find out personal information about them. This assignment will specifically address CLO's 2 and 4.

*Group Presentation – Malware or Data Breach (15%):* The purpose of this assignment is for students to become familiar with some of the most impactful data breaches and malware attacks over the past decade, and who conducted them. In groups of two or three, students will give a 10- to 12-minute presentation on an influential data breach or malware attack. Students will describe the data breach or malware background, the breach/attack itself, who was responsible, and the aftermath of the incident. A more detailed breakdown of the requirements for this assignment can be found on Canvas. This assignment will specifically address CLO's 1, 3, and 5.

*The Threat of Deep Fakes (15%):* The purpose of this assignment is for students to learn how easy/difficult it is to create a deep fake, and the impact they can have on society. Students will have the option of creating a 30 to 60-seconds deep fake video or writing a 4 to 6-page paper (excluding title page and references) on the role of Deep Fakes in facilitating disinformation. This assignment will specifically address CLO's 2 & 3.

*Final Examinations (30%):* Students will be administered a final examination worth 30% of their final grade. The exam will cover material from lectures (including all media presented) and assigned readings**.** The final will be held on the final day of the semester. The exam will be comprised of multiple choice, true/false, and short answer questions. The examinations will specifically address CLO's 1, 2, and 3.

## Grading Information

- In order to receive a grade for this course, all course requirements must be met, and every assignment must be completed. Failure to complete any one assignment may result in a failing grade for this course.
- Individual assignment rubrics will be provided closer to the due date, on Canvas.
- Late assignments/papers will lose 10% for every calendar day that they are late, including weekend days.

### Determination of Grades

| A (plus) | 98% to 100% | A | 95% to <98% | A (minus) | 90% to <95% |
|---|---|---|---|---|---|
| B (plus) | 85% to <90% | B | 78% to <85% | B (minus) | 70% to <78% |
| C (plus) | 67% to <70% | C | 63% to <67% | C (minus) | 60% to <63% |
| D (plus) | 57% to <60% | D | 53% to <57% | D (minus) | 50% to <53% |
| F | Below 50% | | | | |

## University Policies

University-wide policy information relevant to all courses, such as academic integrity, accommodations, etc. will be available on Office of Graduate and Undergraduate Programs' Syllabus Information web page at http://www.sjsu.edu/gup/syllabusinfo/"

# JS 161, Introduction to Cybercrime
## Summer 2022 Course Schedule

*This course schedule is subject to change with fair notice, at the instructor's discretion. All reading assignments listed should be completed prior to class on that date. Additional readings may be assigned.*

| Week | Date | Topics | Readings & Assignments |
|------|------|--------|------------------------|
| **1** | July 5th to July 10th | **The Internet and Crime** - What is Cybercrime - How Cybercrime Functions - The Deep Web | *Readings*     Defining Cybercrime (Payne, 2019)     The Historical Evolutions of Cybercrime (Choi, 2019)     IC3 2020 Report (FBI, 2021)     Exploring the Deep Web (Trend Micro, 2015) |
| **2** | July 11th to July 17th | **Crimes Against the Computer** - Malware - Copyright - Phishing - Botnets - Spam | *Readings*     The Evolution of Cybercrime and Cyberdefense (Trend Micro, 2018)     The Kill Chain (Lockheed Martin, 2015)     MITRE ATT&CK Framework (Petters, 2019)     The Modern Bank Heists (VMWare, 2021) **Tell Me a Story Writing Assignment** (July 17th) |
| **3** | June 18th to July 24th | **Privacy and Security** - Surveillance - Identity Theft - Fraud - Hacking | *Readings*     Technology Use Abuse and Public Perception (Furnell, 2019)     Identity Theft: Nature, Extent, and Global Response (Golladay, 2019)     Private Traits and Atributes are Predictable (Kosinski et al., 2013)     Facebook Studies (Various Authors) **Malware or Data Breach Presentation** (July 24th) |
| **4** | July 25th to July 31st | **Personal Crimes** - Human Trafficking - Cyberbullying - Sex Crimes - Radicalization - Deep Fakes - Fake News | *Readings*     Information Overload Helps Fake News Spread (Menczer & Hills, 2020)     Intimate Partner Violence & the Internet (Clevenger & Gilliam, 2019)     The Past, Present, and Future of Online Child Sexual Exploitation (Westlake, 2019)     The Role of the Internet in Facilitating Violent Extremism and Terrorism (Scrivens, Gill, & Conway, 2019) **Deep Fake or Reflection Assignment** (July 31st) |
| **5** | August 1st to August 5th | **Combating Cybercrime** - Jurisdiction - Police Relations - Digital Forensics - CAN-SPAM | *Readings*     Cybercrime Legislation in the United States (Bossler, 2019)     Forensic Evidence and Cybercrime (Rodgers, 2019)     Digital Forensics (SWGDE, Various)     Police Legitimacy in the Age of Social Media (Nhan-Noakes, 2019) **Final Exam:** (Available August 4th to August 6th) |