

San José State University
Department of Justice Studies
JS 161: Introduction to Cybercrime
Spring 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 (20%): 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 small groups, 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.

Midterm and Final Examinations (40%): Students will be administered a midterm and final examination each worth 20% of their final grade. The exams are closed book and will cover material from lectures (including all media presented) and assigned readings. The midterm will be held during regular class time, while the final will be held during the final exam period. The exams will be comprised of multiple choice 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%
F	Below 60%				

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](http://www.sjsu.edu/gup/syllabusinfo/) at <http://www.sjsu.edu/gup/syllabusinfo/>

JS 161, Introduction to Cybercrime Spring 2021 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
1	01/26/22	Introduction -Course overview -Assignments -Canvas	<i>Articles</i> Historical Evolution of Cybercrime (Choi, Lee, & Louderback, 2019) IC3 2020 Report (FBI, 2021)
2	01/31/22 & 02/06/22	What is Cybercrime -Computer and Internet basics -Cybercrime research -Routine Activity Theory	<i>Articles</i> The Current State of Cybercrime Scholarship (Holt & Bossler, 2014) Defining Cybercrime (Payne, 2019)
3	02/07/22 & 02/13/22	Hacking -Hacker culture -Legal issues -Hacking as a service	<i>Articles</i> What is Hacking (Guru99) The Kill Chain (Lockheed Martin, 2015) MITRE ATT&CK Framework (Petters, 2019)
4	02/14/22 & 02/20/22	Malware -Viruses, worms, trojan horses, rootkits, keyloggers, & ransomware	<i>Articles</i> 2020 Cybersecurity Outlook Report (VMware, 2020) The Evolution of Cybercrime and Cyberdefense (Trend Micro, 2018)
5	02/21/22 & 02/27/22	Privacy & Security -Surveillance -Passwords -Personal safety	<i>Articles</i> Facebook Studies (Various Authors) What is Social Engineering (Webroot) Private Traits and Attributes (Kosinski, Stillwell, & Graepel, 2013)
6	02/28/22 & 03/06/22	Identity Theft & Fraud -Identity theft and fraud -Social media & crime	<i>Articles</i> Identity Theft: Nature, Extent, and Global Response (Golladay, 2019) Police Legitimacy in the Age of Social Media (Nhan & Noakes, 2019) Paper #1 Due: Tell Me a Story (March 6th)
7	03/07/22 & 03/13/22	Deep Web -TOR -Digital currency -The Dark Web	<i>Articles</i> Exploring the Deep Web (Trend Micro, 2015) Cryptocurrency: Enforcement Framework (US DoJ, 2020)
8	03/14/22 & 03/20/22	Email Spam -Legal issues -Legislation efforts -CAN-SPAM -Phishing/pharming	<i>Articles</i> Technology Use Abuse and Public Perception (Furnell, 2019)

Week	Date	Topics	Readings
9	03/21/22 & 03/27/22		Midterm (Available March 21ST to March 25th)
10	03/28/22 & 04/03/22		READING BREAK (No Class)
11	04/04/22 & 04/10/22	Radicalization & Misinformation -Terrorism -Fake news -Deep fakes	<i>Articles</i> Information Overload Helps Fake News Spread (Menczer & Hills, 2020) The Role of the Internet in Facilitating Violent Extremism and Terrorism (Scrivens, Gill, & Conway, 2019)
12	04/11/22 & 04/17/22	Copyright Infringement -What is it? -Who owns the data on the Internet? -Piracy (peer-2-peer)	<i>Articles</i> An Oral History of Napster (Fortune, 2013)
13	04/18/22 & 04/24/22	Sex Crimes -Human trafficking -Child sexual abuse -Sexting -Self-produced & revenge pornography	<i>Articles</i> The Past, Present, and Future of Online Child Sexual Exploitation (Westlake, 2019) Trafficking in Persons Report (Department of State, June 2019)
14	04/25/22 & 05/01/22	Combating Cybercrime - Jurisdiction - Police relations - Digital forensics	<i>Articles</i> Cybercrime Legislation in the United States (Bossler, 2019) Forensic Evidence and Cybercrime (Rodgers, 2019) Police and Extralegal Structures to Combat Cybercrime (Holt, 2019) Group Presentation: Data Breach (Due: May 1st)
15	05/02/22 & 05/08/22	Bullying & Stalking -Online vs offline -Suicide -Law enforcement response	<i>Articles</i> Intimate Partner Violence and the Internet (Clevenger & Gilliam, 2019) Risk and Protective Factors for Cyberbullying Perpetration and Victimization (Wilson, Witherup, & Payne, 2019)
16	05/09/22 & 05/15/22	Digital Forensics -What is it -Prevalence -Best practices -Evidence challenges	<i>Articles</i> Digital Forensics as a Forensic Science Discipline (SWGDE) Collection of Digital and Multimedia Evidence Myths vs Facts (SWGDE) Best Practices for Computer Forensics (SWGDE) Digital and Multimedia Evidence (SWGDE, 2012)
Final Exam	TBD		Final Exam (May TBD)