Cybercrime and Cybersecurity
CRJS 405
(14287)
Kaufman Hall 0100
Tuesday and Thursday, 3:00 – 4:15
Follow the course and the major on Twitter: @ODUcybercrime

Professor Contact
Dr. Rod Graham
rgraham@odu.edu
Batten Arts and Letters 6012
Office Hours: 12:00 – 1:00 on Tuesday and Thursday, and by appointment on Monday and Friday

Course Description

Cybercrime is a growing problem in the United States. In 2016, according to the Internet Crime Complaint Center, US residents reported losing over $1.3 billion because of cybercrime. This course will explore cybercrime through a sociological and criminological perspective. This course has four goals:

1. Students will gain a basic understanding of the architecture of the Internet. Students need knowledge of how computers communicate through interconnected networks in order to grasp how many cybercrimes are committed. They also need to know how to communicate this understanding to the wider population.
2. Students will explore the most common types of cybercrimes. Cybercrimes can be roughly divided into types. One type is the more technical “computer as target” crimes such as hacking and the use of malware, and the second type are the more human-centered “computer as tool” crimes such as romance scams and advance fee frauds.
3. Students will critique the major debates surrounding cybercrime. Our understanding of what should be prohibited and how we should investigate and prosecute cybercrime are continuously being negotiated by groups in society.
4. Students will connect cybercrimes to wider social impacts. While cybersecurity courses may focus more on the concerns of corporations and governments, a cybercrime course focuses more on the individuals and families who are affected by cybercrimes.

Course Materials

Core Reading Materials

1. Yar, Majid. 2013. *Cybercrime and Society*. 2nd Edition. Sage: Thousand Oaks, CA. – This is your main textbook. Your modules are generally ordered by the chapters in this text and it will be the primary content provider.
2. Graham, Roderick. 2014. *The Digital Practices of African-Americans,* Ch. 3. Peter Lang, NY. – This chapter will be used for Module 2.
3. Moore, Robert. 2010. *Cybercrime: Investigating High Technology Computer Crime.* Routledge, NY. – This chapter will be used for Module 11.

Supplemental Material

- This course will incorporate numerous videos and articles as supplements to the main text. Refer to the class schedule at the end of this document for titles.
- Because two of the goals of the course are to critique the debates surrounding cybercrime and to explore wider social impacts, most of the supplemental material is non-academic. You will be exposed to op-ed pieces, industry white papers, and many articles written for a wider audience.

Grading Criteria

Tests – 2 Total - (60%)

- Tests will be delivered online
- Students will have a 4 – 5 day window to complete them.
- Tests will be primarily multiple choice, true-false, and matching and are based on the primary text.
- Test I – Modules 1 – 5
- Test II – Modules 6 – 11

White Paper Assignment - (25%)

- Students will need to produce a 4 – 5 page "white paper" - an evidence based report on a type of cybercrime. This white paper will be composed of:
  - A selected cybercrime
  - A definition of the cybercrime and current trends associated with the cybercrime
  - Two visual aids (graphs, charts, figures) that help the reader understand these trends
  - Suggestions for further reading
  - A glossary of technical terms (between 3 and 10)
  - A reference page (at least three references)
- Students will be able to work in groups up to three. All three students will receive the same score.

Darknet Research Assignment – (15%)

- Students will explore a peer-to-peer, anonymous network and write up their results in a 2 to 3 page paper. The most well-known of these is Tor (https://www.torproject.org/). However, I would urge students to try lesser known networks:
  - Freenet - https://freenetproject.org/
  - Zeronet - https://zeronet.io/
- In your exploration, you need to:
  - Describe in at least two paragraphs how one can access, install, and use the software
  - In 1 – 2 pages, describe the content of the network you chose.
  - Include four captioned screenshots of the network that will act as visual aids and examples for a reader (the screenshots do not count towards the page total).
- Students will be able to work in groups up to three. All three students will receive the same score.

Student Obligations

- If you have a disability or medical condition, which may affect your performance in class, you need to speak with me as soon as possible. Students with disabilities must self-advocate. You will need to provide recent, appropriate documentation, which verifies the need for reasonable academic accommodation.
- Student athletes must provide written verification of your absences in class from your coach. Late notice of absences will not be accepted.
- Students are expected to adhere to the Student Code of Conduct as expressed in your College Student Handbook. In particular, you are expected to engage in the course work with integrity and honesty. Students found guilty of plagiarism will earn a zero for the assignment and sent through the judicial system for further punishment.

Late Assignment/Make-Up Assignment Policy

- Tests and written assignments are completed and submitted online. Students are given at least a 3 – 4 day period in which to complete them. Because of this time frame, excuses are not accepted for work, family emergencies, or simple neglect. A medical excuse can be provided – but it needs to cover the *entire* assignment period.

Course Schedule
(Subject to Change)

Meeting	Date	Topic	Readings and Assignments
1	8/29	Introduction to Class	Yar. Ch. 1 – “Cybercrime and the Internet: An Introduction” [Just Browse] Internet Crime Complaint Center 2016 Report [Video] “Where is Cybercrime Coming From?”
2	8/31	Module 1 - Understanding the Digital Environment Pt. I	The Digital Practices of African-Americans, Ch. 3
3	9/5	Module 1 - Understanding the Digital Environment Pt. I	
4	9/7	Module 2 - Understanding the Digital Environment Pt. II	Four Videos from Code.Org (found on Youtube) 1. “Wires, Cables, and WiFi” 2. “IP Addresses and DNS” 3. “Packets, Routing, and Reliability” 4. “HTTP and HTML” “From Botnet to Malware: a Guide to Decoding Cybersecurity Buzzwords”
5	9/12	Module 2 - Understanding the Digital Environment Pt. II	
6	9/14	Module 3 - Hacking	Yar, Ch. 2 – “Hackers, Crackers, and Viral Coders” “What are Software Vulnerabilities, and Why Are There So Many of Them?” “MalwareTech’s Arrest Sheds Light on the Complex Culture of the Hacking World”
7	9/19	Module 3 - Hacking	
8	9/21	Module 4 - Political Hacking	Yar Ch. 3 – “Political Hacking: From Hactivism to Cyberterrorism” “CyberJihad Hacked US Central Command’s Twitter – How Secure is Your Own Feed?” “‘Burner’ Phones, Social Media and Online Magazines:
9	9/26	Module 4 - Political Hacking	

			Understanding the Technology of Terrorism”
10	9/28	Module 5 - Intellectual Property Theft	Yar Ch.4 – “Virtual ‘Pirates’: Intellectual Property Theft Online” “The Copyright Barons Are Coming. Now’s the Time to Stop Them.” “Copyright Law versus Internet Culture.” [Video] “Blurred Lines Plagiarized”
11	10/3	Module 5 - Intellectual Property Theft	
12	10/5	Unit I Review	White Paper Assignment Due
13	10/12	[No Class]	Unit I Test
14	10/17	Module 6 - Fraud	Yar Ch. 5 – “Cyber-Frauds, Scams and Cons” [Video] Nigerian Love Scam: Frauded and Killed “Why the Victim Can Also Become the Offender in Online Fraud” “The Role of Love stories in Romance Scams: A Qualitative Analysis of Fraudulent Profiles.”
15	10/19	Module 6 - Fraud	
16	10/24	Module 7 - Offensive Content and Hate Speech	Yar Ch.6 – “Illegal, Harmful and Offensive Content Online: From Hate Speech to ‘the Dangers’ of Pornography” “Our Experiments Taught us Why People Troll” “The World May be Headed for a Fragmented “Splinternet””
17	10/26	Module 7 - Offensive Content and Hate Speech	
18	10/31	Module 8 - Child Pornography	Yar Ch. 7 – “Child Pornography and Child Sex Abuse Imagery” “Internet-Facilitated Commercial Sexual Exploitation of Children” “What’s in a Name? Online Child Abuse Material is not ‘Pornography’”
19	11/2	Module 8 - Child Pornography	
20	11/7	Module 9 - Policing the Internet	Yar Ch.9 – “Policing the Internet”

21	11/9	Module 9 - Policing the Internet	“Police Around the World Learn to Fight Global-Scale Cybercrime” “Undercover Online: An Extension of Traditional Policing in the United States.”
22	11/14	Module 10 - Cybercrime and Cyberliberties	Yar Ch. 10 – “Cybercrime and Cyberliberties: Surveillance, Privacy and Crime Control.” [Video] Is the US Government Spying on Me? “Don’t Let Cybercriminals Hide from the FBI” “Warrantless US Spying Is Set to Expire Soon. Let It Die.” “The Attack on Global Privacy Leaves Few Places To Turn.”
23	11/16	Module 10 - Cybercrime and Cyberliberties	
24	11/21	Module 11 – Cybercrime Theory	Moore, Ch. 13 “What is Cybercriminology”?
25	11/28	Module 11 - Cybercrime Theory	
26	12/5	Unit II Review	Darknet Research Assignment Due
27	12/7	[No Class]	Unit II Test