



Machine Learning Techniques Applied to Cybersecurity (ENPM604) Sections 0101 and CY01

Professor: Josef Schaff, D.Sc.
Cell: (301) 904-3759
Email: jschaff@umd.edu
Office Hours: ###

Teaching Assistant: Nikita Patil
Pronouns: ###
Email: ###
Office Hours: ###

Credits: 03

Term: Spring 2024
Course Dates: From Jan 24th – May 9th

Course Times: Tuesdays 7:00 pm - 9:40 pm
Classroom: ###

Canvas/ELMS: ###

Course Description

This course covers an extensive amount of ML and applications to Malware analysis, some network traffic analysis and memory forensics. These areas within cyber security often require analysts to process vast amounts of data (and meta-data) to discover relevant patterns and/or anomalies. The growth of malware and ubiquity of IoT devices result in an ever-increasing amount of data, where the demand for analysis of the data can far outstrip the supply of available (and qualified) human analysts.

In this course, we will introduce students to relevant unsupervised and supervised Machine Learning techniques (e.g., clustering and classification) that can be applied to Cyber Security problems. We will show and demonstrate how to transform big security-data challenges into information asymmetry advantages on the side of the defender by leveraging these techniques. In particular, we will discuss and demonstrate via labs how clustering algorithms can be leveraged to identify malware among a large set of binaries and explore how developing approximate versions of clustering algorithms can allow us to further improve performance without adversely affecting accuracy.

Many of the examples (and labs) in the first half of the course will use ScikitLearn libraries, as these are well-vetted and have good descriptions. The student is encouraged to review topics on this site beyond what is covered in this course.

We will also discuss and demonstrate how classification algorithms that include Logistic Regression and Support Vector Machines can be utilized to develop models that we can train to identify malicious behavior exhibited in host and network data collected using memory forensics and network capture tools. With respect to vulnerability detection, we will explore how neural networks can be applied to problems such as vulnerability research to generate fuzzing inputs in an automation fashion to improve code coverage and uncover vulnerabilities in a target binary. There are new aspects that need to be covered with respect to ML and cyber, so most of this material will be used as a foundation for newer algorithms. Some topics include graph NNs and Transformers, and references to many algorithms for detecting anomalies, and managing unbalanced data sets. ***As a culmination for this course each student will put together an informal research paper on a novel ML-Cyber topic. The purpose of this is to allow each student to develop expertise in a niche area within ML-enabled cyber, focused upon the latest research.***

Prerequisites

We will assume that each student has a basic understanding of core computer engineering concepts and is comfortable with programming in general (python for the example labs). Exposure to machine learning concepts and techniques can be helpful but are not necessary.

Learning Outcomes

After successfully completing this course, you will be able to:

- Apply relevant machine learning techniques to problems across various areas within the cyber security domain that include malware analysis, memory forensics, network traffic analysis, and vulnerability research.
- Use multiple approaches to transform cyber security data (and metadata) into a mathematical representation (i.e., vector) suitable for ingesting by Machine Learning algorithms.
- Develop methods to select, implement, and modify appropriate algorithms that are suitable for the cyber security application of interest.
- Research and investigate late-breaking methods in ML and their application to cyber. Ideally, each student will develop the beginnings of their unique expertise in a subtopic of their choosing for ML-cyber applications.
- Understand cyber resilience, and how to survive or outwit a threat.

Course Materials

Readings:

1. C. Chio and D. Freeman, (2018). Machine learning and security: Protecting systems with data and algorithms. O'Reilly Media.
2. Raschka, S. & Mirjalili, V. (2019). Python machine learning- Third Edition. Packt Publishing Ltd.
3. Many papers to be supplied on Canvas.

Hardware/Software:

You should have a basic knowledge of Python, and can use the python development environment of your choice, provided that it supports the majority of related tools, e.g., NumPy, Pandas, etc. Virtualbox is the preferred tool to run a Virtual Machine for the labs since it is free. Please download it at the following link and install:
<https://www.virtualbox.org/wiki/Downloads>.

Course Structure

This course includes both on-campus and online sections. **To attend synchronously online, log into ELMS-Canvas at the time of the Section 0101 class [Tuesdays 7:00 pm - 9:40 pm] and select "Video Conference" from the left side menu.** This will open a Zoom link to the live classroom.

For asynchronous online students, all lectures will be recorded and made available on ELMS-Canvas under “Panopto Recordings/Video Lectures” within 24 hours of the class time. Be sure to review the recorded lecture in a timely manner.

On-campus students come to class prepared to engage with the lecture and materials. Online students, be sure to log into Canvas regularly and participate in discussions and activities. Regardless of the section you are enrolled in, participation is expected.

Please note that F1 students enrolled in the on-campus section are required to attend in person. If you have a conflict on a particular day, please reach out to me in advance to discuss.

Communication Guidelines

Communicating with the Instructor

My goal is to be readily available to you throughout the semester. **I can be reached by email at jschaff@umd.edu.** Please DO NOT email me with questions that are easily found in the syllabus or on ELMS-Canvas (e.g., When is this assignment due? How much is it worth? etc.), but please DO reach out about personal, academic, and intellectual concerns/questions.

While I will do my best to respond to emails within 24 hours, you will more likely receive email responses from me on weekends. Please also contact the Teaching Assistant for any questions, or if you have to urgently get hold of me.

When constructing an email to me please put “ENPM XXXX (Section XXXX): Your Topic” in the subject line. This will draw my attention to your email and enable me to respond to you more quickly.

Additionally, please review [These tips for 'How to email a Professor'](#). By following these guidelines, you will be ensured to receive a timely and courteous response.

Finally, if you need to discuss issues not appropriate for the classroom and/or an email, we can arrange to talk by phone, over Zoom, or in person. Send me an email asking for a meeting and we can set something up.

Announcements

I will send IMPORTANT messages, announcements, and updates through ELMS-Canvas. To ensure you receive this information in a timely fashion, make sure your email and announcement notifications (including changes in assignments and/or due dates) are enabled in ELMS-Canvas ([How to change notification settings in CANVAS](#)).

Log into our ELMS-Canvas course site at least once every 24-hour period to check your inbox and the Announcements page.

Names/Pronouns and Self-Identifications

The University of Maryland recognizes the importance of a diverse student body, and we are committed to fostering inclusive and equitable classroom environments. I invite you, if you wish, to tell us how you want to be referred to in this class, both in terms of your name and your pronouns (he/him, she/her, they/them, etc.). Keep in

mind that the pronouns someone uses are not necessarily indicative of their gender identity. Visit trans.umd.edu to learn more.

Additionally, it is your choice whether to disclose how you identify in terms of your gender, race, class, sexuality, religion, and dis/ability, among all aspects of your identity (e.g., should it come up in classroom conversation about our experiences and perspectives) and should be self-identified, not presumed or imposed. I will do my best to address and refer to all students accordingly, and I ask you to do the same for all of your fellow Terps.

Communicating with your Peers

With a diversity of perspectives and experience, we may find ourselves in disagreement and/or debate with one another. As such, it is important that we agree to conduct ourselves in a professional manner and that we work together to foster and preserve a virtual classroom environment in which we can respectfully discuss and deliberate controversial questions. I encourage you to confidently exercise your right to free speech—bearing in mind, of course, that you will be expected to craft and defend arguments that support your position. Keep in mind, that free speech has its limit and this course is NOT the space for hate speech, harassment, and derogatory language. I will make every reasonable attempt to create an atmosphere in which each student feels comfortable voicing their argument without fear of being personally attacked, mocked, demeaned, or devalued.

Any behavior (including harassment, sexual harassment, and racially and/or culturally derogatory language) that threatens this atmosphere will not be tolerated. Please alert me immediately if you feel threatened, dismissed, or silenced at any point during our semester together and/or if your engagement in discussion has been in some way hindered by the learning environment.

Netiquette Policy

Netiquette is the social code of online classes. Students share a responsibility for the course’s learning environment. Creating a cohesive online learning community requires learners to support and assist each other. To craft an open and interactive online learning environment, communication has to be conducted in a professional and courteous manner at all times, guided by common sense, collegiality and basic rules of etiquette.

Grading

Grade Breakdown

Assignment	Percentage %
Labs	20%
Background Survey for Research Topic	20%
Exams (2 each worth 20%)	40%
Research Project and Paper	20%
Total	100%

Course Assignments

Labs

There are 4 programming labs that are exercises only – you will be graded on performing the labs to the best of your ability, and is collectively worth 20% of each student's grade. Note that each student is expected to perform lab work individually and with no collaboration, unless otherwise explicitly announced.

Show that you did the lab work and what you have concluded (even if you don't entirely solve it).

If a lab section fails to run (e.g., run-time error, syntax error, etc....) on the grader's VM, describe what you encountered and learned in the process.

Background Survey of Potential Research – the “proposal stage” for one or more topics that you plan to explore.

A background survey of potential research areas that cover ML-cyber applications will be presented by each student and briefly discussed with the class. Individuals can ultimately select a topic for their final term paper described by any other student, provided that your research is unique only to you – this is ideally so that you gain an expertise in a unique area which makes you highly valued by organizations looking for a new approach to their ML-cyber approaches. Guidelines for the research requirements (i.e., questions that you will answer in your research) is provided in a document called “Research paper requirements description-ENPM604”. You can not answer all of the questions at this stage, but are expected to answer them in your final project.

Exams

There will be two take home exams worth 20% each, that will each cover material from Module I, and Modules II & III, respectively.

Research Project – the final project that answers all the required questions.

A Research project on a new area of ML-cyber research where you will develop the expertise (i.e., your niche area for this course). The project will be discussed briefly during the first class, and in more detail around the time of midterm. Follow the guidelines and answer all the questions in the document “Research paper requirements description-ENPM604”.

Grading of Assignments

All assignments will be graded according to a predetermined set of criteria (i.e., rubric) which will be communicated to students before the assignment is submitted.

To progress satisfactorily in this class, students need to receive timely feedback. To that end, **it is my intention to grade all assignments within 10 days of their due date.** If an assignment is taking longer than expected to grade, students will be informed of when they can expect to see their grade.

Grade Computation

All assessment scores will be posted on ELMS/Canvas page. If you would like to review any of your grades (including the exams), or have questions about how something was scored, please email me to schedule a time for us to meet and discuss.

It is expected that you will submit work by the deadline listed in the syllabus and/or on ELMS-Canvas. Late work will be penalized according to the late work policy described in the **Course Policies and Procedures** section below.

Grade Disputes: I am happy to discuss any of your grades with you, but please contact the TA first. If one of us has made a mistake, we will immediately correct it. **Any formal grade disputes must be submitted in writing and within one week of receiving the grade.**

Final letter grades are assigned based on the percentage of total assessment points earned. To be fair to everyone I have to establish clear standards and apply them consistently, so please understand that being close to a cutoff is not the same as making the cut (89.99 \neq 90.00). It would be unethical to make exceptions for some and not others.

Final Grade Cutoffs									
+	95.00%	+	85.00%	+	75.00%	+		+	
A	92.00%	B	82.00%	C	72.00%	D	<70%	F	<60.0%
-	90.00%	-	80.00%	-	70.00%	-		-	

Course Schedule

Approximate dates only and subject to change!!!

Key Date	Event	Topic	Duration	Description
Week 1	Lecture 1	Introduction	Course 1 hour	Motivating the need for applying machine learning techniques to cyber security applications
	Lecture 2	Revised State of the Art in Applying Machine Learning to Cyber Security	1.5 hours	Cyber ML data vs. autonomous sensor data: unbalanced data and anomaly detection. Survey of machine learning techniques currently being explored in academia and industry to address cyber security problems. We will discuss several papers related to the latest methods (graphNN, transformers, etc.).
Module I: Introduction to Machine Learning (Weeks 1-6)				
	Lecture 3	Revised Machine Learning Overview and anomaly detection	0.5 hour	Overview of the three types of machine learning (i.e. supervised learning, unsupervised learning, and reinforcement learning). Discussion of the steps needed to build machine learning systems.

Week 2	Lecture 4	Revised Simple Machine Learning Algorithms and Classifiers	1 hours	Laying the groundwork for advanced machine learning algorithms by first introducing the perceptron and adaptive linear neurons.
	Lecture 5	Revised Machine Learning Classifiers: Support Vector Machines (SVM)	1 hours	SVM is another widely used classification algorithm that is very powerful and can also be viewed as an extension of the perceptron (<i>discussed in Lecture 4</i>). We will discuss key concepts that include separating hyperplanes and kernelization.
	Lab 1a	Classification	10 min	(Classifier) Identify the best tuning parameters for a subset of classifiers against a supplied data set
Week 3	Lecture 5 (cc'd)	Machine Learning Classifiers: Support Vector Machines (SVM)	1 hours	
	Lecture 6	Machine Learning Classifiers: Logistic Regression	1 hour	Logistic regression is one of the most widely used classification algorithms in industry and is similar to the perceptron and adaptive linear neurons previously discussed.
	Lecture 7	Machine Learning Classifiers: Decision Trees and Forests	30 minutes	Discuss algorithms for building decision trees along with the splitting criteria. In addition, we will discuss how multiple decision trees can be combined via random forests
Week 4	Lecture 8	Clustering Algorithms: K-means	30 minutes	Introduction to one of the most popular clustering algorithms and understanding the strengths and challenges of using this algorithm. In particular, we will discuss the importance of specifying k, the number of clusters, and also the challenges of choosing an appropriate k.
	Lecture 9	Clustering Algorithms: Agglomerative Hierarchical	30 minutes	In contrast to k-means, agglomerative hierarchical clustering algorithms do not require k to be specified. We will discuss the tradeoffs (that include performance) of this algorithm with respect to k-means.
	Lab 1b	Clustering	10 min	(Clustering) Implement an approximate hierarchical clustering algorithm and compare its performance versus k-means implemented using the sci-kit learn on a supplied data set.
	Lecture 10	Revised Clustering Algorithms- Nearest Cluster Search w/ Logarithmic Time Complexity. Graph NNs as solutions to mapping dependencies / similarities.	1.5	Finding cluster nearest to a datapoint of interest with logarithmic (versus linear) average search complexity using a binary tree-based approach. Description of Graph NNs as solutions to mapping dependencies / similarities.

Week 5	Guest Lecture	Reinforced Learning	2.0 hour	Reinforced Learning – methods and applied algorithms.
	Lecture 11	Revised Dimensionality Reduction via Principal Component Analysis (PCA)	0.5 hour	We will motivate why data compression techniques can significantly increase performance of ML algorithms. We will also discuss the fundamental concepts underlying PCA and the steps to extract the principal components.

Week 6	New Lecture	Cognitive Architectures	1	Cognitive Architectures: SOAR / ACT-R / Overall impacts and utility.
	Lecture 12/13 + mostly new	Adversarial Machine Learning	1 hour	Revised Adversarial Machine Learning Building cyber-resilient ML architectures
	Toolkits		0.5 hour	Toolkits like PYOD, NN arch simulators, Neuromorphic / SNNs HW = Akida brainchip, TinyTile, etc.

Module II: Unsupervised Learning Applied to Cyber Security (Weeks 6-11)

	Exam I Q&A	Exam I Q&A	30 min	
Week 7	Exam 1	**Class will be on Zoom**		Module I Material
Week 8	Lecture 14	Network Traffic Analysis	1.5 hours	Revised Discussion of techniques for applying unsupervised ML to network traffic analysis problems. How the Radial Basis Function (RBF) NN does first-stage unsupervised learning.
	Lecture 15	Malware Analysis	30 minutes	We will explore unsupervised ML malware analysis techniques that include how vex intermediate representation (IR) can be utilized to perform code slice emulation and call trace analysis to generate data about the binary's run-time behavior

Week ?	Spring Break	N/A	N/A	N/A
Week 9	Lecture 15 (cc'd)	Malware Analysis	1 hour	We will explore unsupervised ML malware analysis techniques that include how vex intermediate representation (IR) can be utilized to perform code slice emulation and call trace analysis to generate data about the binary's run-time behavior

Lecture 16	Revised Expressing executable binaries (and associated meta-data) in a mathematical representation	30 min		We will discuss techniques for representing binaries and associated meta-data in a mathematical representation (e.g. vector) suitable for ingesting into ML algorithms.
			Lab 2a	Malware Detection w/ Approximate Hierarchical clustering techniques 15 minutes Develop a detection tool that can ingest a set of binaries and use clustering techniques to identify anomalous binaries.
			Lecture 17	Binary Similarity Analysis 45 min Introduce methods and techniques for analyzing similarity of basic blocks, functions, and binaries.
Week 10 (4/05)			Lecture 18	Advanced Binary Analysis Overview 1 hour Overview of advanced binary analysis techniques that can be leveraged to

				generate binary meta-data for purposes that include malware analysis
	Lecture 19	VEX Intermediate Representation Language	30 min	An intermediate representation that allows for advanced analysis of binaries in an architecture agnostic manner
	Labs 2a & 2B	2a = Due Sat. 4/8 and 2b = Due Mon. 4/17	15 mins	Review Lab 2b
Module III: Supervised Learning Applied to Cyber Security (Weeks 11-13)				
Week 11	<i>Revised</i> Lecture 22 but mostly new material	Malware Detection w/ classification Time-domain classifiers RNNs, LSTMs, GRUs. Next-gen Reservoir computing.	2.5 hours	Techniques to delineate malware from benign software
Week 12	Exam 2			Includes all Module II & III Material up to and including Lecture 22
Week 13	New Material	Generative AI/ML and how it fits cyber & Network Forensics	2.5 hours	Methods will include GANs, Autoencoders, LLMs.
Week 14 and Week 15	Research paper <i>short presentations</i>		2.5 hours X2	Final paper presentations. If time available future advanced topics will be discussed.

(Due last day of class)

Final presentations / paper due.

Note: This is a tentative schedule, and subject to change as necessary – monitor the course ELMS page for current deadlines. In the unlikely event of a prolonged university closing, or an extended absence from the university, adjustments to the course schedule, deadlines, and assignments will be made based on the duration of the closing and the specific dates missed.

Course Policies and Procedures

The University of Maryland’s conduct policy indicates that course syllabi should refer to a webpage of course-related policies and procedures. For a complete list of graduate course related policies, visit the [Graduate School website](#). Below are course-specific policies and procedures which explain how these Graduate School policies will be implemented in this class.

Satisfactory Performance

The Graduate School expects students to take full responsibility for their academic work and academic progress. The student, to progress satisfactorily, must meet all the academic requirements of this course. Additionally, each student is expected to complete all readings and any preparatory work before each class session, come to class prepared to make substantive contributions to the learning experience, and to proactively communicate with the instructor when challenges or issues arise.

Questions about Assignments

Please ask all questions you may have about an assignment **by 7:00 PM the day before the assignment is due**. Any questions asked after that time may not be answered in time for you to make changes to your work.

Late Work Policy

Assignments should be completed by the due date and time listed with the assignment, on the syllabus, and/or in the course calendar. If you are unable to complete an assignment by the stated due date, it is your responsibility to contact your instructor to discuss an extension, **at least 24 hours BEFORE the assignment is due**. Extensions are not guaranteed, but may be granted at the instructor's discretion.

Assignments submitted late will receive a 10% deduction in total grade per each calendar day late up to a maximum of three days late (i.e., there is a maximum of a 30% grade reduction for assignments submitted late). Work submitted more than three days late will not receive feedback and will automatically earn a grade of zero.

Religious Observance

It is the student's responsibility to inform the instructor of any intended absences for religious observances in advance. **Notice should be provided as soon as possible but no later than the end of the schedule adjustment period.**

Academic Integrity

For this course, some of your assignments will be collected via Turnitin on ELMS/Canvas. I have chosen to use this tool because it can help you improve your scholarly writing and help me verify the integrity of student work. For information about Turnitin, how it works, and the feedback reports you may have access to, visit [Turnitin Originality Checker for Students](#)

The University's Code of Academic Integrity is designed to ensure that the principles of academic honesty and integrity are upheld. In accordance with this code, the University of Maryland does not tolerate academic dishonesty. Please ensure that you fully understand this code and its implications because all acts of academic dishonesty will be dealt with in accordance with the provisions of this code. All students are expected to adhere to this Code. It is your responsibility to read it and know what it says, so you can start your professional life on the right path. **As future professionals, your commitment to high ethical standards and honesty begins with your time at the University of Maryland.**

It is important to note that course assistance websites, such as CourseHero, or AI generated content are not permitted sources, unless the instructor explicitly gives permission. Material taken or copied from these sites can be deemed unauthorized material and a violation of academic integrity. These sites offer information that might be inaccurate or biased and most importantly, relying on restricted sources will hamper your learning process, particularly the critical thinking steps necessary for college-level assignments.

Additionally, students may naturally choose to use online forums for course-wide discussions (e.g., Group lists or chats) to discuss concepts in the course. However, **collaboration on graded assignments is strictly prohibited unless otherwise stated**. Examples of prohibited collaboration include: asking classmates for answers on quizzes or exams, asking for access codes to clicker polls, etc. Please visit the [Office of Graduate Studies' full list of campus-wide policies](#) and reach out if you have questions.







Finally, on each exam or assignment you must write out and sign the following pledge: **"I pledge on my honor that I have not given or received any unauthorized assistance on this exam/assignment."**

If you ever feel pressured to comply with someone else's academic integrity violation, please reach out to me straight away. Also, **if you are ever unclear** about acceptable levels of collaboration, **please ask!**

IMPORTANT: In this class, plagiarism will not be tolerated, which extends to the labs. **Significant chunks of code copied for use in the labs without citing the source is an example of plagiarism. Plagiarism also includes (but is not limited to) running someone else's code through an obfuscation engine and submitting that code as your own.**

Each person is expected to write the research papers and code for the labs themselves. Submitting code that you weren't the author of or code where significant chunks that you were supposed to implement were not authored by you is against course policy. This will also result in an automatic 0. All research sources (including ChatGPT) must be listed in the references for your paper – format is not critical.

To help you avoid unintentional violations, **the following table** lists levels of collaboration that are acceptable for each graded exercise. Each assignment will contain more specific information regarding acceptable levels of collaboration.

	 OPEN NOTES	 USE BOOK	 LEARN ONLINE	 GATHER CONTENT With AI	 ASK FRIENDS	 WORK IN GROUPS
Labs	✓	✓	✓	---	---	---
Background Research Topic	✓	✓	✓	✓	✓	--✓-
Exams	✓	✓	✓	---	---	---
Final Project	✓	✓	✓	✓	✓	✓

Course Evaluation

Please submit a course evaluation through Student Feedback on Course Experiences in order to help faculty and administrators improve teaching and learning at Maryland. All information submitted to Course Experiences is confidential. Campus will notify you when Student Feedback on Course Experiences is open for you to complete your evaluations at the end of the semester. Please go directly to the [Student Feedback on Course Experiences](#) to complete your evaluations. By completing all of your evaluations each semester, you will have the privilege of

accessing through Testudo the evaluation reports for the thousands of courses for which 70% or more students submitted their evaluations.

Copyright Notice

Course materials are copyrighted and may not be reproduced for anything other than personal use without written permission.

Tips for Succeeding in this Course

1. **Participate.** I invite you to engage deeply, ask questions, and talk about the course content with your classmates. You can learn a great deal from discussing ideas and perspectives with your peers and professor. Participation can also help you articulate your thoughts and develop critical thinking skills.
2. **Manage your time.** Students are often very busy, and I understand that you have obligations outside of this class. However, students do best when they plan adequate time that is devoted to course work. Block your schedule and set aside plenty of time to complete assignments including extra time to handle any technology related problems.
3. **Login regularly.** I recommend that you log in to ELMS-Canvas several times a week to view announcements, discussion posts and replies to your posts. You may need to log in multiple times a day when group submissions are due.
4. **Do not fall behind.** This class moves at a quick pace and each week builds on the previous content. If you feel you are starting to fall behind, check in with the instructor as soon as possible so we can troubleshoot together. It will be hard to keep up with the course content if you fall behind in the pre-work or post-work.
5. **Use ELMS-Canvas notification settings.** Pro tip! Canvas ELMS-Canvas can ensure you receive timely notifications in your email or via text. Be sure to enable announcements to be sent instantly or daily.
6. **Ask for help if needed.** If you need help with ELMS-Canvas or other technology, IT Support. If you are struggling with a course concept, reach out to me and your classmates for support.

Student Resources and Services

Taking personal responsibility for your learning means acknowledging when your performance does not match your goals and doing something about it. I hope you will come talk to me so that I can help you find the right approach to success in this course, and I encourage you to visit the [Counseling Center's Academic Resources](#) to learn more about the wide range of resources available to you. Below are some additional resources and services commonly used by graduate students. For a more comprehensive list, please visit the Graduate School's [Campus Resources Page](#).

Accessibility and Disability Services

The University of Maryland is committed to creating and maintaining a welcoming and inclusive educational, working, and living environment for people of all abilities. The University of Maryland is also committed to the principle that no qualified individual with a disability shall, on the basis of disability, be excluded from participation in or be denied the benefits of the services, programs, or activities of the University, or be subjected to discrimination. The [Accessibility & Disability Service \(ADS\)](#) provides reasonable accommodations to qualified individuals to provide equal access to services, programs and activities. ADS cannot assist retroactively, so it is generally best to request accommodations several weeks before the semester begins or as soon as a disability

becomes known. Any student who needs accommodations should contact me as soon as possible so that I have sufficient time to make arrangements.

For assistance in obtaining an accommodation, contact Accessibility and Disability Service at 301-314-7682, or email them at adsfrontdesk@umd.edu. Information about [sharing your accommodations with instructors, note taking assistance](#) and more is available from the [Counseling Center](#).

Writing Center

Everyone can use some help sharpening their communication skills (and improving their grade) by visiting [The Graduate School's Writing Center](#) and schedule an appointment with them. Additionally, international graduate students may want to take advantage of the Graduate School's free [English Editing for International Graduate Students \(EEIGS\) program](#).

Health Services

The University offers a variety of physical and mental health services to students. If you are feeling ill or need non-emergency medical attention, please visit the [University Health Center](#).

If you feel it would be helpful to have someone to talk to, visit [UMD's Counseling Center](#) or [one of the many other mental health resources on campus](#).

Notice of Mandatory Reporting

Notice of mandatory reporting of sexual assault, sexual harassment, interpersonal violence, and stalking: As a faculty member, I am designated as a "Responsible University Employee," and I must report all disclosures of sexual assault, sexual harassment, interpersonal violence, and stalking to UMD's Title IX Coordinator per University Policy on Sexual Harassment and Other Sexual Misconduct.

If you wish to speak with someone confidentially, please contact one of UMD's confidential resources, such as [CARE to Stop Violence](#) (located on the Ground Floor of the Health Center) at 301-741-3442 or the [Counseling Center](#) (located at the Shoemaker Building) at 301-314-7651.

You may also seek assistance or supportive measures from UMD's Title IX Coordinator, Angela Nastase, by calling 301-405-1142, or emailing titleIXcoordinator@umd.edu.

To view further information on the above, please visit the [Office of Civil Rights and Sexual Misconduct's](#) website at ocrsm.umd.edu.

Basic Needs Security

If you have difficulty affording groceries or accessing sufficient food to eat every day, or lack a safe and stable place to live, please visit [UMD's Division of Student Affairs website](#) for information about resources the campus offers you and let me know if I can help in any way.

Veteran Resources

UMD provides some additional supports to our student veterans. You can access those resources at the office of [Veteran Student life](#) and the [Counseling Center](#). Veterans and active duty military personnel with special

circumstances (e.g., upcoming deployments, drill requirements, disabilities) are welcome and encouraged to communicate these, in advance if possible, to the instructor.