# CPSC 585 - Artificial Neural Networks

Project 4, Spring 2021

due April 7

*Last updated Monday March 15, 10:00 pm PDT*

[Adversarial machine learning](https://en.wikipedia.org/wiki/Adversarial_machine_learning) is an interesting topic in both machine learning and security research that is not covered in the textbook. The goal of an adversarial attack is to purposely craft feature vectors that will be misidentified by a classifier.

In this project you will research the topic and write a brief paper summarizing what you have learned.

The project may be completed individually, or in a group of no more than three students.

## Requirements

Your paper should be three full pages of text, typed double-spaced (approximately 750-1000 words) for individuals and pairs, and five full pages (1250-1500 words) for teams of three. A fourth page should list references.

### Works Cited

* Cite 3-5 sources of information on adversarial machine learning in addition to the Wikipedia article linked above.
  + At least one source should be a current news article on the topic.
  + At least two of the sources should be peer-reviewed academic papers.
* Use [ACM](https://www.acm.org/publications/authors/reference-formatting) or [IEEE](https://ieee-dataport.org/sites/default/files/analysis/27/IEEE%20Citation%20Guidelines.pdf) citation format.

## Tips

* Adversarial examples are *not* the same as Generative Adversarial Networks (GANs), which are covered in Chapter 10 of the textbook.
* Be careful to [evaluate your sources](https://libraryanswers.fullerton.edu/faq/197540) carefully before using them as the basis for your paper. Be particularly wary of content on blogs such as *Towards Data Science*. While these can be a valuable way to begin your research, they tend to recycle content and may not be careful about citing sources.
* Look for survey or review papers in journals such as [*ACM Computing Surveys*](https://dl.acm.org/journal/csur), [*Computer Science Review*](https://www.journals.elsevier.com/computer-science-review), and [*Foundations and Trends in Machine Learning*](https://www.nowpublishers.com/MAL).
* Search the [ACM Digital Library](https://dl-acm-org.lib-proxy.fullerton.edu/), [IEEE Xplore](https://ieeexplore-ieee-org.lib-proxy.fullerton.edu/search/advanced), and [Safari Books Online](https://learning-oreilly-com.lib-proxy.fullerton.edu/home/) for additional sources of information.

## Submission

Submit your paper in PDF through Turnitin on Canvas before class on the due date.

If the assignment is completed by a team, only one submission is required. Be certain to identify the names of all students on your team in the paper’s header. See the following sections of the Canvas documentation for instructions on group submission:

* [How do I join a group as a student?](https://community.canvaslms.com/t5/Student-Guide/How-do-I-join-a-group-as-a-student/ta-p/468)
* [How do I submit an assignment on behalf of a group?](https://community.canvaslms.com/t5/Student-Guide/How-do-I-submit-an-assignment-on-behalf-of-a-group/ta-p/294)