Skills for Impact: Digital Security and Human Rights

2021 Spring Term

Instructor: Cameran Ashraf, Ph.D. Office: 247
Email: AshrafC@spp.ceu.edu Office Hours: TBA

Course Description

Around the world activists, human rights defenders, and journalists, face unprecedented intrusion and surveillance into their activities on the Internet. These intrusions can range from passive surveillance to active infiltration and ultimately can lead to imprisonment, the chilling of opposition voices, and the dismantling of civil society.

This course will build on the topics discussed in the course: The Internet & Human Rights by exposing students to a hands-on practicum of the challenges and opportunities human rights defenders, activists, journalists, and other threatened individuals face around the world. Students will learn digital security tactics, strategies, and understand the importance of operational security and digital security hygiene to better examine and relate to the myriad of threats to human rights online.

Learning Outcomes

By the end of this course students will:

1. Build on theory and case studies by engaging with specific tools and technologies;
2. Be able to take concrete steps towards enhancing digital security, understanding online threat environments;
3. Understand, communicate, and implement these new skills to individuals, groups, and organizations through direct hands-on work

Course Texts

Any course texts will be posted on the class website. Students are strongly encouraged to print out the readings instead of reading from their computers. Reading a physical copy contributes to superior comprehension. Printing out copies of the readings can be done at computer labs or the SPP main office.

Course Structure

This course is an intensive three-day seminar and workshop. You will be expected to participate fully in course activities. What you get out of this class will be precisely what you put into it.

Attendance

Due to the intense delivery format of the SFI modules, student absence is not permitted. If students miss a significant portion of an SFI course due to an excused absence, no credit will be awarded and the student

will receive a "withdraw" (or "WN") on their transcripts. In the event students are absent for a significant portion of an SFI without an excused absence, an "F" will be given.

Assignments - <u>Please note that all papers will be submitted through the TurnItIn system!</u>

According to the CEU Student Rights, Rules, and Academic Regulations (Annex 1.), in case of a 2-credit course, students are expected to spend 80-100 hours on non-classroom, autonomous, self-directed learning (homework, consultations with the course instructor and preparing for classes).

<u>Participation</u>

This course has a strong participation component, and you are expected to participate, discuss, and ask questions about the topics and activities at every class meeting. If you are uncomfortable doing this, please consider dropping the course as it is an important component of your grade.

<u>Threat Model</u>

REQUIRED. When doing sensitive work, it is vital to understand the threat landscape in which you or your organization are operating. This can range from threats which are located entirely on the Internet to threats located offline who seek to get your online data. Students will be expected to <u>fully</u> complete a threat model worksheet with in-depth discussion of each element of their threat model.

<u>Digital Security Action Plan (maximum 1,800 words)</u>

REQUIRED. Students will be expected to prepare a Digital Security Action Plan informed by a threat model and the class topics. This will include: 1) Development and description of a hypothetical scenario relevant to student research or interests; 2) a FULL threat model; 3) discussion of plan implementation and feasibility.

<u>Policies</u>

- All university policies relating to plagiarism, cheating, harassment, etc. will be fully enforced.
- SPP policy is to fail students with more than one unexcused absence for a 2-credit course and more than two unexcused absences for a 4-credit course. Alternatively, final grades may be lowered in proportion to unexcused absences.
- Be respectful to yourself, other students, and to the professor.
- I am an understanding individual. If there are things happening in your life which may prevent you from being successful in class, please come speak with me. I am on your side.
- The instructor reserves the right to change this syllabus at any time.

Breakdown of final pass/fail grade:

Participation =	**35%**
Threat Model =	**20%**
Digital Security Action Plan =	**45%**

Class Schedule

Session 1 (May 31 / 9:00 AM – 5:10 PM): Introduction & Threat Models

Class introductions, course outline, discussion of structure and objectives. Overview of topic. Relevant film and discussion.

9 – 10 AM: Introductions, discussion of course structure, objectives, and expectations.
10-10:10 AM: Break
10:10 – 11:30 AM: Human Rights & Technology Movie: Black Code OR Burma VJ OR The Cleaners
11:30 AM – 1 PM: Lunch
1 – 2:30 PM: Threat Landscape & Student Threat Discussion
2:30-2:40 PM Break
2:40 – 4:40 PM Threat model development
4:40 – 5:10 PM Reflections & Discussion

Session 2 (June 1 / 9:00 AM – 5:10 PM): Basics of Digital Security

Developing a security mindset based on threat modelling, basics of web browsing and social media security.

9 – 10:20 AM: Discussion and reflections on previous day. Digital Operational Security Mindset & Begin phishing exercise.
10:20 – 10:30 AM: Break
10:30 – 11:30AM: Continue phishing exercise.
11:30 AM – 1 PM: Lunch
1 – 2:30 PM: Continue and Present Results of Phishing Exercise
2:30-2:45 PM Break
2:45 – 4:40 PM Password Security
Exercise: Secure password generation, presentation
4:40 – 4:50 PM Break
4:50 – 5:10 PM Reflections & Discussion

Session 3 (June 2 / 9:00 AM – 5:10 PM): Advanced Topics

Advanced topics including encrypted email, secure browsing and censorship circumvention.

9 – 9:30 AM: Discussion and reflections of previous days. Recap if needed.
9:30 – 10:30 Circumvention & secure browsing
Exercise: Install and use TOR & Brave browser & Plugins
10:30 - 10:40 AM: Break
10:40 - 11:40 AM: Begin Email Security
Exercise: Send an encrypted email
11:40 AM – 1 PM: Lunch
1:00 - 2:00 PM Continue Email Security // Begin Digital Security Action Plan
2:00 - 2:10 PM Break
2:10 - 5:10 Continue Digital Security Action Plan
Exercise: Present Digital Security Action Plan
5:00 – 5:10 PM: Conclusion