Term Information

Effective Term	Spring 2026

General Information

Course Bulletin Listing/Subject Area	Cyber Security
Fiscal Unit/Academic Org	Engineering Administration - D1400
College/Academic Group	Engineering
Level/Career	Undergraduate
Course Number/Catalog	2111
Course Title	Social Engineering: Spams, Scams, and Saving your Assets
Transcript Abbreviation	Social Engineering
Course Description	Cyberspace connects people and technology, but humans often misunderstand this ecosystem, leaving them vulnerable to Social Engineering. Students will learn about social engineering tactics, manipulation, and defense strategies and the ethical use of this knowledge. Students will be taught to create their own presentation to train a demographic to detect, avoid, and defend against such attacks.
Semester Credit Hours/Units	Fixed: 3

Offering Information

Length Of Course	14 Week
Flexibly Scheduled Course	Never
Does any section of this course have a distance education component?	No
Grading Basis	Letter Grade
Repeatable	No
Course Components	Lecture
Grade Roster Component	Lecture
Credit Available by Exam	No
Admission Condition Course	No
Off Campus	Never
Campus of Offering	Columbus

Prerequisites and Exclusions

Prerequisites/Corequisites	None
Exclusions	None
Electronically Enforced	Yes

Cross-Listings

Cross-Listings

Subject/CIP Code

Subject/CIP Code	11.1003
Subsidy Level	Baccalaureate Course
Intended Rank	Freshman, Sophomore, Junior, Senior

Requirement/Elective Designation

Lived Environments

Course Details

Course goals or learning objectives/outcomes

- Have an understanding of social engineering in their own lived environment – including the methodology and psychology of it
- Understand the ethical implications of social engineering and learn the legal consequences of some real world examples
- Learn how targeted populations are manipulated and what they can do to protect themselves
- Gain the knowledge to recognize and avoid scams, to protect their digital footprint, and teach others to do the same
- Know how to change their behaviors to mitigate their risks
- Work with their team to develop a persuasive and educational presentation for a specific demographic
- Present to a pre-arranged group of the demographic (approximately 20-30 people)

Content Topic List

- Introduction to the class, basics of information security
- Social Engineering Introduction
- Psychology of Deception
- Demographic Worldview
- Common Social Engineering Tactics
- Recognizing and Avoiding Scams
- Protecting Your Digital Footprint
- Social Engineering in the workplace
- Emerging Threats
- Bringing it all together
- Finalizing and presenting

Sought Concurrence

No

Attachments

- NC_CYBRSEC_2111_Syllabus_GE_ELO_SL_High_Impact.pdf: Instructor Syllabus

  (Syllabus. Owner: Quinzon-Bonello,Rosario)

- CybrSec 2111 Syllabus.pdf: Syllabus

  (Syllabus. Owner: Quinzon-Bonello,Rosario)

- CybrSec 2111 GE - lived environments submission.pdf: Theme Worksheet

  (Other Supporting Documentation. Owner: Quinzon-Bonello,Rosario)

- CybrSec2111 Course Schedule.pdf: Course Schedule

  (Other Supporting Documentation. Owner: Quinzon-Bonello,Rosario)

- CybrSec2111 service-learning-inventory HIP form.pdf: HIP Form

  (Other Supporting Documentation. Owner: Quinzon-Bonello,Rosario)

- Revisions based on Committee Feedback.pdf: Revisions

  (Other Supporting Documentation. Owner: Quinzon-Bonello,Rosario)

- CybrSec 2111 GE - lived environments submission.pdf: Revision Theme Worksheet

  (Other Supporting Documentation. Owner: Quinzon-Bonello,Rosario)

- CybrSec 2111 Syllabus.pdf: Revision Syllabus

  (Other Supporting Documentation. Owner: Quinzon-Bonello,Rosario)

Comments

- Per email w/ R. Quinzon-Bonello 09-05-2025, changed CH to 3 from 4 and removed HIP Service Learning designation. *(by Steele,Rachel Lea on 09/05/2025 03:58 PM)*
- Instruction submitted three revised documents. *(by Quinzon-Bonello,Rosario on 08/08/2025 10:08 AM)*
- Please see feedback email sent 5-19-25. *(by Neff,Jennifer on 05/19/2025 11:48 AM)*
- Please remember to upload the GE form, the High Impact Practice form, and the schedule for the course. *(by Vankeerbergen,Bernadette Chantal on 04/22/2025 12:52 PM)*

Workflow Information

Status	User(s)	Date/Time	Step
Submitted	Quinzon-Bonello,Rosario	04/22/2025 09:40 AM	Submitted for Approval
Approved	Quinzon-Bonello,Rosario	04/22/2025 11:59 AM	Unit Approval
Approved	Quinzon-Bonello,Rosario	04/22/2025 12:00 PM	College Approval
Revision Requested	Vankeerbergen,Bernadette Chantal	04/22/2025 12:52 PM	ASCCAO Approval
Submitted	Quinzon-Bonello,Rosario	05/02/2025 11:27 AM	Submitted for Approval
Approved	Quinzon-Bonello,Rosario	05/02/2025 11:27 AM	Unit Approval
Approved	Quinzon-Bonello,Rosario	05/02/2025 11:27 AM	College Approval
Revision Requested	Neff,Jennifer	05/19/2025 11:48 AM	ASCCAO Approval
Submitted	Quinzon-Bonello,Rosario	08/08/2025 10:08 AM	Submitted for Approval
Approved	Quinzon-Bonello,Rosario	08/08/2025 10:08 AM	Unit Approval
Approved	Quinzon-Bonello,Rosario	08/08/2025 10:08 AM	College Approval
Pending Approval	Jenkins,Mary Ellen Bigler Hilty,Michael Neff,Jennifer Vankeerbergen,Bernadette Chantal Steele,Rachel Lea	08/08/2025 10:08 AM	ASCCAO Approval

#	Committee Comment	Response
1.00	The reviewing faculty voted not to approve the High-Impact Practice designation. Please see below for next steps and options for moving forward:	
2.00	At this time, the service-learning element of the course does not meet the expectations of the service-learning High-Impact Practice. The service component appears to consist of a one-time presentation to members of the demographic at a student's location. For the activity to qualify as service-learning, it must involve sustained engagement that is driven by the community's needs. Should the unit continue to seek approval as a High-Impact Practice course, the syllabus and supporting documents should provide more information about the nature of the community partners, how the demographic is defined, and how student engagement is consistent and informed by community input. Additionally, if students are expected to conduct a focus group as part of their presentation, it should be clearly indicated how they will be taught to ethically conduct this type of research.	Will not resubmit as a HIP Service Learning course
3.00	As described, the HIP activity may align more appropriately with the Research and Creative Inquiry High-Impact Practice, unless the course is revised to include deeper community partnership. However, the reviewing faculty encourage the unit to focus on resubmission as a 3-credit hour course in the Lived Environments Theme. HIP approval could follow after the course demonstrates strong alignment with the Theme.	Will not resubmit as a HIP Service Learning course
4.00	Please note, should the unit continue to seek the service-learning HIP, "S" should be added as a suffix to the course number ("2111S") in curriculum.osu.edu and on the syllabus, as this is the designation for service-learning courses.	Will not resubmit as a HIP Service Learning course
5.00	As mentioned above, the reviewing faculty encourage the unit to focus on resubmission as a 3-credit hour course in the Lived Environments Theme by addressing the following feedback in a revision:	ICDT Leadership determined it is best to resubmit this as a 3 credit hour GE course with an optional lab available in the future
5.01	The reviewing faculty request that the Lived Environments Goals and ELOs be stated in the syllabus along with a brief explanatory paragraph summarizing how the course meets the Goals and ELOs. The Lived Environments Goals and ELOs can be found in an easy to copy/paste format on the Arts and Sciences Curriculum and Assessment Services website.	Added to the overall description of how this course connect with the Lived Environments Theme. Also added descriptions in the Course Schedule which helps to describe this connection.

5.02	The reviewing faculty are concerned that the course, in its current form, does not sufficiently meet the expectations of the Theme. More explicit connections are needed between course content and the Theme specific Goals and ELOs (3.1-4.3). The syllabus and supporting documents are vague and do not clearly indicate how students will engage with the complexity, uncertainty, and historical change that are central to the Theme. To strengthen alignment, the reviewing faculty request that the syllabus and GE submission form be revised to do the following:	summary of the following
5.03	More clearly articulate how the course moves beyond foundation learning and fosters depth in analyzing both digital and real-world environmental change over time and across spatial contexts.	Additional descriptions added to each week describing the purpose and the concepts and considering their own behavior in different platforms which makes them susceptible to attack
5.04	Foster critical engagement with the logic and assumptions underpinning key course concepts (e.g., how different groups perceive and respond to online threats) in order to incorporate a more nuanced, evidence-based approach.	Descriptions added to the Course schedule, now in the syllabus, which defines the purpose of the section, better articles which help students to understand the section, and anchor with real world examples. The 4 quizzes are replaced by Essay assignments for students examine and demonstrate their own comprehension of the reading material and the reading for each period.
5.05	Explicitly outline how students will examine the social, cultural, and political factors shaping digital behavior and perception.	Students will not only learn how the demographic's behaviors and their worldview which makes them susceptible to social engineering attacks and add to their knowledge and understanding through the interviews and the focus group. Assigned reflections for each of these requires students to examine and report on these behaviors and perceptions. The Course Schedule provides a description which outlines how the students will accomplish the social, cultural, and political factors shaping digital behavior and perception.
5.06	Clarify how students will engage with underlying frameworks (e.g., surveillance, power, and access, that structure digital discourse) of the Theme.	Asking how this interacts with the other concepts and concerns. How are they relating to others? Think of ICS. Also think of the other lived environments such as as a student, employee, social

5.07	The reviewing faculty request that the assignment descriptions in the syllabus have clearer alignment with the ELOs to ensure students are not only engaging with Theme concepts but are applying them in rich ways.	The syllabus now has a section for the assignments. Each assignment has a description
5.08	To help demonstrate how the course builds toward achieving the Theme ELOs, the reviewing faculty request that the course calendar in the syllabus be revised to indicate how each class session will engage with Theme content.	"Theme Engagement" added to each section of the course calendar. This lists the ELOs met and provides a summary of how it meets those.
5.09	The reviewing faculty note that the assigned readings in the course schedule consist of introductory-level materials and lack the depth expected at the advanced Themes level. They request that the course include more rigorous, peer-reviewed scholarly sources (e.g., journal articles) that are not necessarily more technical, but rather offer an in-depth exploration of the Theme.	Added to the Syllabus "Assignments & Grading" section. More articles added pertaining to the subject in focus for each period of the class and added how each week is meeting the ELOs
5.10	The reviewing faculty request that the syllabus include descriptions that clearly explain the expectations of each assignment. They also request that both the syllabus and GE submission form make it clear how the assignments (especially the presentation) support engagement with the Theme. Currently, the assignments seem to have a relatively narrow and technical focus, with limited connection to the broader social and environmental contexts of the Theme.	Expand the syllabus to include the assignments and provide a detailed description of the assignments, including how it is supporting the Lived Environments theme. Also added the assignments to the ELO in the submission
5.11	The reviewing faculty request that the scaffolding of the assignments in the course be strengthened. For example, the three reflection papers are a valuable component, but they currently account for 10% of the final grade each and may not allow for deep engagement. The reviewing faculty suggest that instead, one of these reflections (perhaps the one focused on “how the demographic feels targeted”) be expanded into a more substantive research-based assignment that incorporates peer-reviewed sources. Additional low-stakes assignments leading up to the major papers could help students develop the skills needed for successful completion of the bigger assignment.	Change quizzes to Comprehension Essay Assignments to have students think about the topics of the prior 2 sections (typically 2) and modified the Reflections order to build upon each other and added one more reflection at the end of the class.
	The reviewing faculty request that the reference to the Embedded Literacies be removed from the syllabus, as this is often confusing to students. [Syllabus p. 1]	corrected
	The reviewing faculty note that the language for the Title IX statement appears in the syllabus twice, once under the heading “Title IX” and once under the heading “Sexual Misconduct.” The reviewing faculty recommend removing the latter from the syllabus. [Syllabus p. 5]	corrected
	The reviewing faculty recommend that the unit use the most recent version of the university’s diversity statement if they wish to keep it in the syllabus. The updated statement can be found in an easy to copy/paste format on the Office of Undergraduate Education website. [Syllabus pp. 5-6]	corrected

	The reviewing faculty recommend that the unit update the links in the Title IX and religious accommodations statements due to the recent renaming of the Office of Institutional Equity to the Office of Civil Rights Compliance. The full statements with the updated links can be found in an easy to copy/paste format on the Office of Undergraduate Education website. [Syllabus pp. 5-6]	corrected
	The reviewing faculty recommend that the unit use the most recent version of the Student Life Disability Services statement, which can be found in an easy to copy/paste format on the Office of Undergraduate Education website. [Syllabus pp. 6-7]	corrected
	The reviewing faculty request that a cover letter be provided that details all changes made as a result of their feedback.	Will provide a summary based on this spreadsheet
	The reviewing faculty encourage the unit to reach out to Brian Lower.30 (faculty Chair of the Theme Advisory Group for Lived Environments) and Meg Daly.66 (Associate Dean of Undergraduate Education) to schedule a meeting to discuss how to best address the above feedback.	Done

CYBRSEC 2111 – Social Engineering: Spams, Scams, and Saving Your Assets

Course Information

- Course Days
  - 2 80-minute classes
  - Credit hours: 3
  - Mode of delivery: In person
- Theme
  - Lived Environments

> *"There is no technology today that cannot be defeated by social engineering."*
> *-Frank Abagnale*

Instructor

- Name: Roland Kreml
- Email: Kreml.1@osu.edu
- Office hours:

Teaching Assistant

- Name: TBD
- Email:
- Office Hours:

Course Description

Cyberspace is a lived environment that unites humans and technologies. Education, entertainment, news, social media, medical and financial information, and more are available in this vast environment where humans sometimes spend more time than their offline lives. Humans often perceive of this cyber ecosystem in naive ways, leaving them vulnerable and easily manipulated by other humans in methods known as "Social Engineering" (SE). This very phrase, "social engineering" suggests the merging of the technical world—engineering—with the human digital ecosystem.

To understand this world, one needs to apply an interdisciplinary framework that can capture the complex relationships of humans to their cyber environments. How do people adapt to this environment and develop good cyber-hygiene to be able to safely exist in this environment?

Humans can respond to and shape their environments through proactive steps, and in this course students will be educated about SE attack methods, how people are manipulated, how to protect themselves, and how to communicate this issue to others. Students who know how to identify attacks and to protect themselves will be better netizens of the online world, more capable of understanding how individual behaviors can have systemic consequences. In turn, this makes graduates a lower risk and a better choice for employers.

Students will come away from this class with not only a sound understanding of how to detect, and avoid SE in their daily and work lives, but also how to coach others to do the same.

Course Objective

> *"While we teach, we learn."*
> *-Seneca*

This course explores SE and its influence on digital and real-world lived environments. Students will start by learning basic security concepts and the SE concept. As SE is largely a manipulation, students next will learn about psychology of deception and a demographic expert will teach them the worldview of their demographic to help them frame how cybercriminals manipulate people based on their habits, trusting behavior, and needs. They will next learn about the specific tactics social engineers use and how it is performed in social media and the workplace. The student will round out their knowledge by learning how to protect themselves, recognize, and avoid attacks.

Parallel to learning about SE, the students will work in groups of 3-4 students to develop a persuasive presentation. Students will first learn how to create a persuasive presentation and use this and their growing knowledge about SE to develop their first draft of their presentations which they will record and receive feedback from classmates. The teams will use this feedback to revise their presentations and add more information learned from instruction. They will then present to focus groups to receive feedback from the target focus group.

After this process of crafting, receiving feedback, and refining their presentations the course concludes with students presenting to educate a specific demographic (arranged by the instructor) about the danger of social engineer and how that demographic can protect themselves.

By understanding how digital and real-world environments impact and are impacted by human interactions, trust, and security practices, students will come away from this course with a sound understanding of how to detect and avoid SE attacks in their work and daily lives. Additionally, they will be able to teach others to do the same.

Course Goals

After successfully completing this course, a student will:

1. Have an understanding of SE in their own lived environment – including the methodology and psychology of it,
2. Learn how targeted populations are manipulated and what they can do to protect themselves,
3. Gain the knowledge to recognize and avoid scams, to protect their digital footprint, and teach others to do the same,
4. Understand how they are susceptible to SE attacks,
5. Know how to change their behaviors to mitigate their risks,
6. Work with their team to develop a persuasive and educational presentation for a specific demographic,
7. Receive feedback from classmates to improve their delivery, and
8. Understand the ethics and legal responsibilities of SE

Course Prerequisites

There are no prerequisites for this class.

Attendance

Attendance is critical in this class – this is ***not*** an online course. I will post lecture slides on Carmen prior to lectures; however, they do not replace the assigned reading nor the lectures. Attendance will be important to completion of assignments as it will for exams.

If you miss a class, you are responsible for getting notes and information missed from your fellow classmates – get to know your classmates – or come to my office hours to answer questions you may have.

Attendance is recorded for all classes. Your attendance is a major factor in my flexibility of your end grade. I do understand situations arise throughout the semester and you are permitted 2 missed classes without any loss in attendance score.

I will perform in-class, non-graded, lessons-learned checks in each class. Along with this is an attendance check. This is done in TopHat, available in Carmen. Make sure TopHat is working on your preferred device.

Discussion Boards and Peer Reviews

Discussion Boards will not be required in this class. Students will perform reviews of 2 other team's online submission.

Assignments & Grading

Reflections Assignments:

- Student's vulnerability to SE (Individual assignment)
    - Based on what students have learned through in class instruction and assigned reading about SE attacks and the psychology of the attacks, students will introspectively analyze their own vulnerabilities to SE, how they possibly have been exploited by at attack and what they should do to mitigate their risks.
- Student's implicit bias to the demographic (Individual assignment)
    - Student's will use knowledge from in-class instruction and assigned reading about the world-view of different demographics and the concept of implicit bias to reflect how they have an implicit bias toward those demographics and how those biases impact their own actions and relations.
- How the demographic is, and feels, targeted (Individual assignment)
    - Students will research their assigned demographic:
        - how there are susceptible,
        - how their worldview impacts their vulnerability,
        - how hackers use environmental stresses such as deadlines, bills, medicine, school, job, and others to manipulate their demographic
        - how the threat to this demographic has changed with the development of smartphones, tablets, and Internet of Things (IOT devices such as smart homes), and AI. Students will utilize instruction, and assigned reading, and their own research to develop what they should do to protect themselves.
    - Students will then interview a person in that demographic to learn about their worldview and what they do to protect themselves and will develop a report of their research and their interview, including what they advised the person should do to protect themselves.

- Final thoughts (Individual assignment)
    - Each student will create a reflection of what they understood about SE and their vulnerabilities prior to the class, what they learned, what they will do different, and how they will advise their friends and families to protect themselves.

Presentation assignments

- Record a presentation about their demographic (Group assignment)
    - Students will be grouped with 3 other students in the class based on their assigned demographic. Working in teams, students will share and discuss their "How a demographic feels targeted" with their team members and work as a team to develop and record a presentation of how their team's assigned demographic is vulnerable to SE, the methods of attack, and mitigation techniques as well as how the demographic is influenced by social, media, and political rhetoric.
    - Each member will also perform a peer view of their teammates as part of this assignment.
- Inter-Team Feedback (Individual assignment)
    - Each student will review presentations from 2 teams (not their own) and provide constructive feedback.

Comprehension Essay Assignments evaluating student's comprehension of the assigned reading and instruction during the period

- Weeks 1-3
- Weeks 4-5
- Weeks 7-8
- Weeks 9-12

Exams

- Midterm exam covers weeks 1-5
- Final exam comprehensive for major Midterm topics, but mostly covers weeks 6-13

Assignments, exams, and presentations will be assigned a letter grade from A to E. Rubrics will be included on all assignments. Any journals, papers, attendance and participation are also considered for the final adjusted grade. The possibility of extra credit or make-up projects will be determined at a later date.

Students will be evaluated as follows:

Topic	% of grade	Points
Attendance	4%	40
4 Comprehension Essay assignments	16%	160
Reflections (30% total) • Student's implicit bias • How the demographic is, and feels, targeted • Student's vulnerability to SE and how to protect themselves • Final thoughts of what they have learned and how they will change	 8% 8% 15% 4%	 80 80 150 40
Presentation • Pre-recorded demographic presentation • Peer review team members	 14%	 140
Peer review of 2 teams	4%	40
Midterm exam	12%	120
Final Exam	15%	150

Total		1000

Lived Environments Theme Expected Learning Outcomes (ELOs)

Although not the traditional lived environment, cyberspace is a lived environment that unites humans and technologies and this course, Social Engineering: Spams, Scams, and Saving Your Assets, teaches students about the tactics and techniques hackers use to manipulate people in their on-line world to make errors which result in significant losses and stress. Social Engineering lived environments have dynamic demographics based on work, social, age, sex, culture, and even relationship status and individuals may defend well in platforms like Carmen and Email, but may be more susceptible in their Social Media lived environment due to perceived peer pressure or fear of missing out (FOMO).

ELO 1.1 Engage in critical and logical thinking.

Today's student reside as much in the online environment as they do in their physical environment. They are subject to many threats and this course will provide the students the understanding of social engineering, and the methodology and psychology of it. Students will hear from cybersecurity, psychology, and demographic experts to help them understand the threat for themselves and for others. They will learn how targeted populations are manipulated and what they can do. Through this education, they will develop critical and logical thinking of how to discern social engineering attacks and protect themselves. By the end of this course they will be able to recognize tactics of social engineers, and not only how they should respond to these attacks to protect themselves, but also how they can teach others to do the same.

ELO 1.2 Engage in an advanced, in-depth, scholarly exploration of the topic or ideas within this theme.

Through the reading, exercises, and instruction, students will have a good understanding of the threat of social engineers and will be able to apply this understanding of how they and others are manipulated within their online environment. Through reflection assignments, students will identify their own susceptibility to being manipulated and their vulnerability to social engineering and will examine the consequences on their information and through the essay assignments (formerly quizzes) they will contemplate and demonstrate their understanding of the assigned readings and instruction.
They will use what they have learned in class and work in a 3-4 person team of students develop a persuasive presentation.

ELO 2.1 Identify, describe, and synthesize approaches or experiences.

Lecture Course materials support the learning of basic cybersecurity and psychology concepts relevant to social engineering and their online presence, including:

- Tactics of a social engineer
- How to recognize and avoid scams.
- How to protect their digital footprint.
- Social Engineering in social media, the workplace, and other sources.
- How to coach others about identifying potential threats.

Reading

All material used for this class is freely available. Each module provides important reading material to expose students to concepts prior to the instruction and set the basis of learning of the topic.

Reflections

Students will reflect upon:

- Their implicit bias: Students will learn about the psychology of social engineering and how about their own implicit bias toward the specific demographic and how those biases can be used in social engineering attacks. Students will reflect how this made them understand their implicit bias and what they can do about it.
- How an assigned demographic is, and feels targeted.
- Their own Vulnerabilities to social engineering: Students will learn methods of social engineering attacks and will identify their own vulnerabilities to social engineering.
- Final thoughts of what they have learned and what they will change

Knowledge checks and assessments
At the end of each class will be knowledge checks performed in TopHat. These knowledge checks are not graded but will identify where students may not understand the content and to encourage additional conversation. Each module builds upon understanding of prior course topics, so Comprehension Essay Assignments are used to evaluate understanding of material and concepts.

ELO 2.2 Demonstrate a developing sense of self as a learner through reflection, self- assessment, and creative work, building on prior experiences to respond to new and challenging contexts.
Students will have multiple activities to develop their sense of self through this course. Reflection assignments are intentionally scaffolded to help students understand more as the course continue – not only of the content, but also of their perceptions. Comprehension Essay assignments will require students to introspectively consider what they have learned and how it pertains to them. Open discussions in class will also allow open reflection. Students will work in a team to build their persuasive presentation designed for a specific demographic which they will receive feedback from other students.

ELO 3.1 Engage with the complexity and uncertainty of human- environment interactions.
The topic of social engineering is fraught with complexity and uncertainty of human-environment interaction. Social Engineering is the soft-underbelly of the hardened shell of cybersecurity. Throughout this course, students will hear about the psychology, demographics, and cybersecurity integration of Social Engineering which will expose the students to the mindset of hackers and how people are manipulated in the cyber lived environment. Students will be assigned to talk to a member of the assigned demographic that additional information will aid to develop and deliver a persuasive presentation.
Four assignments will lead students to research and consider this topic:
1) Student's vulnerability to social engineering,
2) Students implicit bias to the demographic,
3) How the demographic is, and feels, targeted
4) Final thoughts of what they have learned and how they will change

ELO 3.2 Describe examples of human interaction with and impact on environmental change and transformation over time and across space.
Students will learn about how humans interact with the cyber environment by hearing examples of social engineering attacks. They will hear the history of social engineering attack in the early days of individual, less sophisticated attacks to the complicated and enterprise-developed turn-key social engineering attacks available for hire and now the developing use of AI for attacks. They will learn the importance of education and how it can change the outcome to protect this soft under-belly. Comprehension Essay assignments will require student to consider the human interaction, how it has changed, how they threats have changed, and what should be done. Through this course students will lower their risk and their future employers as they will have better security awareness. They will have

the knowledge to become change agents for their in-real-life (IRL) friends, family, business, classmates, and colleagues.

ELO 4.1 Analyze how humans' interactions with their environments shape or have shaped attitudes, beliefs, values and behaviors.
Students will read, learn, and discuss attack methods and their growing sophistication. Students will reflect on these through reflection assignments and the Comprehension Essay assignment including methodology to shape attitudes.

ELO 4.2 Describe how humans perceive and represent the environments with which they interact.
Students will learn that the perception of the online world varies across the demographics, but there is a recurring theme: People are skeptical to believe many sources in today's world. Hackers know a well-crafted phish which targets their income, life, or family and people are willing to believe anything. Students will learn the more educated people become the more likely they will be able to recognize and avoid the attack and they will learn how to be the change agents in their different lived environments. The assigned readings are in place to identify how humans perceive and represent the multiple environments they interact which are susceptible to SE attacks.

ELO 4.3 Analyze and critique conventions, theories, and ideologies that influence discourses around environments.
In this course students will learn more about their own lived environment and how their own actions may make them more and others vulnerable. Students will hear about tactics, information, and disinformation which contribute to fear, uncertainty, and doubt. These result in reactive and possibly detrimental actions. Education is the solution and by completing this course students will be better equipped to identify and protect themselves against attacks and will be able to educate others to do the same. Students will explore this in all of their reflections and the Comprehension Essay Assignment of weeks 7-8 and 9-12

Grade Disputes

I am happy to revisit grades and to discuss the evaluation of your work with you. Please make grade change requests in-person (during office hours) or send to my Carmen email. Please be ready to outline where you believe you should have received additional points and how many points you should have received.

Course Materials, Fees, and Technologies

Required Books
There is no required textbook. All required materials will be made available on the course website through links and PDFs.

Course technology
- If students do not have computer when they deliver their presentation, a computer will be available.
- Microsoft PowerPoint is the expected presentation application.

Required technical skills this course

- Basic computer and web-browsing skills
- Familiarity with PowerPoint
- Navigating Carmen. For questions about specific functionality, see the Canvas Student Guide. Additional navigation instructions are provided within the course.

Required equipment and software

- Microsoft Office 365, specifically, PowerPoint
  - All Ohio State students are eligible for free Microsoft Office 365 ProPlus through Microsoft's Student Advantage program. Full instructions for downloading and installation can be found at go.osu.edu/office365help.
- Computer or tablet (current Mac (OS X), PC (Windows 7+), iPad) to develop their PowerPoint presentation

Course Schedule

Week 1: 2 days

Introductions, About the class and assignments, and how to succeed. Basics of Information Security

Preread

- Syllabus and Carmen Modules
- Chapters 1, 2, 6 https://www.mitnicksecurity.com/the-history-of-social-engineering

Assignment:

Determine who you want to partner with for the presentation

Assignment due:

None

Theme integration: Overview of the goal and purpose of the class and assignments. How their online presence is multiple lived environments, based on their own roles and demographics

Week 2: 2 days

Social Engineering Introduction

Preread

- Human Cognition Through the Lens of Social Engineering Cyberattacks: https://pmc.ncbi.nlm.nih.gov/articles/PMC7554349/
- An interdisciplinary view of social engineering: A call to action for research: https://www.sciencedirect.com/science/article/pii/S2451958821000749
- https://www.mitnicksecurity.com/blog/ways-hackers-use-social-engineering-to-trick-your-employees

Assignment:

None

Assignment due:

None

Theme integration: ELO 1.1, 1.2, 3.1, 4.1

This begins setting the foundation of this course and helping students understand, introspectively, their multiple environments which they "live" as a student, employee, family member, socially with their friends/culture, and other demographically lived environments which they may temporarily or permanently reside. Students will be exposed to studies which identify demographics and the methods which attackers will use to manipulate people in their online lived environment. These touch on the

concepts of these manipulations such as conformity, likability, fear of missing out(scarcity), imitation, emotions, quid pro quo, authority, and even boredom as well as the different demographics which people fit in their online lived environments.

Week 3: 2 days

Psychology of Deception and the Ethics of Social Engineering

Preread

- Amygdala Hijacking and Social Engineering: https://www.social-engineer.org/social-engineering/amygdala-hijacking-and-social-engineering/
- A Study on the Psychology of Social Engineering-Based Cyberattacks and Existing Countermeasures: https://www.mdpi.com/1677374
- Psychology of Cybersecurity and Human Behavior: https://identitymanagementinstitute.org/psychology-of-cybersecurity-and-human-behavior/
- Creating a Code of Ethics for Social Engineering in Cybersecurity: A Case Study: https://ojs.victoria.ac.nz/wfeess/article/view/7671/6807

Assignment:

- **Week 1-3 Comprehension Essay Assignment:** Understanding of the instruction and assigned reading

Assignment due:

- Partners for presentations (otherwise randomly assigned)

Theme Integration: ELO 1.1, 1.2, 2.1, 3.2, 4.1, 4.2

The assigned readings introduce students to the concepts of the psychological manipulation at the core of SE attacks. In addition, it explores the human interaction factor and how we have learned to transform the environment to better defend against attack and develop education so people are aware of what makes them vulnerable and to be able to recognize attacks to prevent it before it has a chance to land. The essay assignment will require students to analyze and critique what was in place prior to the attack and how that change.

Week 4: 2 Days

Demographic Worldview

Preread

- https://www.ncbi.nlm.nih.gov/books/NBK589697/
- https://kirwaninstitute.osu.edu/implicit-bias-module-series
- Effects of Demographic Factors on Phishing Victimization in the Workplace: https://www.researchgate.net/publication/356750869_Effects_of_Demographic_Factors_on_Phishing_Victimization_in_the_Workplace

Assignments:

- **Reflection #1: Your Implicit Bias results.**

Assignment due:

- Week 1-3 Comprehension Essay Assignment

Theme Integration: ELO 1.1, 1.2, 2.1, 2.2, 3.1, 4.1, 4.2

The assigned readings educate students about the viewpoint for different demographic and how their beliefs and attitudes are manipulated in the world of SE. The Reflection builds upon the new concept learned in class about implicit bias to help students further introspect their own implicit bias toward demographics.

Week 5: 2 Days
Common Social Engineering Tactics

Preread

- Chapter 3: https://www.mitnicksecurity.com/the-history-of-social-engineering
- Psychological Exploitation of Social Engineering Attacks: https://www.cyber-risk-gmbh.com/Psychological_Exploitation_of_Social_Engineering_Attacks.html

Assignment:

- **Weeks 4-5 Comprehension Essay Assignment: Understanding of instruction and assigned reading**

Assignment due:

- Reflection #1: Your Implicit Bias results

Theme Integration: ELO 1.1, 1.2, 2.2

This section is mostly focused on the social engineering tactics and engages the students in advanced exploration of the tactics used for SE attack. The Essay Assignment leads students to demonstrate their developing understanding of SE and the world view of demographics.

Week6: 2 Days
Midterm Study and Exam

Preread

- Study Guide

Assignment:

- None

Assignment Due

- Weeks 4-5 Comprehension Essay Assignment

Theme Integration:

Evaluation of student learning

Week 7: 2 Days
Recognizing and Avoiding Scams

Preread

- Chapter 4: https://www.mitnicksecurity.com/the-history-of-social-engineering
- Social Engineering Attack Mitigation: https://www.researchgate.net/publication/307606034_Social_Engineering_Attack_Mitigation

Assignment:

- **Reflection #2: How the demographic is, and feels, targeted**

Assignments due:

- None

Theme Integration: ELO 1.1, 1.2, 2.1, 2.2, 3.1, 3.2, 4.1, 4.2, 4.3

This section, with the assigned reading, in class instruction, and the Reflection, touches on all ELO requirements as this is continuing the critical thinking and then turn this toward how the focus demographic is aware of their vulnerability to the threats in the environment the live in the daily actions. They will continue this analysis in the reflection to analyze their actions making them vulnerable and critique their current and their prior sources of discourses in their environment.

Week 8: 2 Days
Protecting Your Digital Footprint

Preread

- https://www.identityguard.com/news/how-to-protect-your-digital-footprint
- Systematic Review on Social Engineering: Hacking by Manipulating Humans: https://www.scirp.org/html/5-7800712_106599.htm
- How to Manage Your Digital Footprint for 2025: 20 Tips for Students: https://research.com/education/how-to-manage-digital-footprint

Assignment:

- **Reflection #3: Student vulnerability to social engineering and how to protect themselves**
- **Weeks 7-8 Comprehension Essay Assignment: Understanding of instruction and assigned reading**

Assignments due:

- Reflection #2: How the demographic is, and feels, targeted

Theme Integration: ELO 1.1, 1.2, 2.1, 2.2, 3.1, 3.2, 4.1, 4.2, and 4.3

This follows the same reasoning for the previous theme integrations, except the students will turn this analysis to themselves: What are they doing in their multi-faceted online presence; What interactions make them vulnerable to known, previously unknown, and future threats; What uncertainties and concerns do they have; What do they hear from their families, friends, and others who influence them which may make them more vulnerable; What will they change to become more aware and to protect themselves; and What will they do to educate others?

Week 9: 2 Days
Social Engineering in Social Media & designing an effective presentation

Preread

- Chapter 5 and 7: https://www.mitnicksecurity.com/the-history-of-social-engineering
- Designing an effective presentation -
- https://journals.plos.org/ploscompbiol/article?id=10.1371/journal.pcbi.1009554

Assignment:

- **Develop and record demographic presentation with assigned team**

Assignment due:

- Weeks 7-8 Comprehension Essay Assignment: Understanding of instruction and assigned reading

Theme Integration: ELO 1.1, 1.2, 2.1, 2.2, 3.1, 3.2, 4.1, 4.2, 4.3

The topics of the lectures educate students about the presence in social media which makes them vulnerable. The assignment to develop a presentation brings together the concepts learned in this course. Students will work with their team to review what they have learned about their respective demographics and use their collective understanding along with what they have learned and reflected upon up to this point to begin developing a presentation intended for their team's assigned demographic.

Week 10: 2 Days
Social Engineering in the Workplace

Preread

- Social Engineering Susceptibility: A Study on Demographics and Information Security Awareness in Small Businesses: https://acbspjournal.org/2023/07/11/social-engineering-

susceptibility-a-study-on-demographics-and-informationsecurity-awareness-in-small-businesses

- Falling for phishing attempts: An investigation of individual differences that are associated with behavior in a naturalistic phishing simulation: https://www.sciencedirect.com/science/article/pii/S0167404823002237

Assignment:

- None

Assignment due:

- **Reflection #3: Student vulnerability to social engineering and how to protect themselves**

Theme Integration: ELO 1.1, 1.2, 2.1, 2.2, 3.1, 3.2

This lecture focuses on the manipulation which occurs in the workplace. It continues to build their knowledge and understanding of how a person is tricked through SE which compromises them as an employee. Through this education students will be able to see another facet of SE and how they need to be aware of it even in their work. This scaffolded knowledge allows the teams to continue to build more content for their presentation assignment.

Week 11: 2 Days

Major social engineering events and what could have been done to prevent them

Preread

- Social Engineering in Non-Linear Warfare: https://mds.marshall.edu/cgi/viewcontent.cgi?article=1000&context=jade
- Nation-State Cyber Attacks on Critical Infrastructure: A Case Study and Analysis of the 2014 Sony Pictures Hack by North Korea: https://www.researchgate.net/publication/387465146_Nation-State_Cyber_Attacks_on_Critical_Infrastructure_A_Case_Study_and_Analysis_of_the_2014_Sony_Pictures_Hack_by_North_Korea
- Twitter Investigation Report: https://www.dfs.ny.gov/Twitter_Report

Assignment:

- None

Assignment due:

- None

Theme Integration: ELO 3.2, 4.1, 4.2, 4.3

Students will hear examples of SE attacks and how people were manipulated. They will learn about decisions made which made it possible and the decisions made which mitigate the risk of future successful attacks. The classes will be highly interactive to discuss what happened and how students have seen similar events that they may have recognized at the time, or after reading the assigned reading they realize what was in progress.

Week 12: 2 Days

Emerging Threats

Guest Speaker: Cybersecurity Expert

Preread

- The Future of Social Engineering: https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/the-future-of-social-engineering

Assignment:

- **Peer review of 2 teams' videos**
- **Weeks 9-12 Comprehension Essay Assignment: Understanding of instruction and assigned reading**

Assignment Due:

- Demographic presentation recording

Theme Integration: ELO 1.1, 1.2, 3.1, 3.2, 4.1, 4.2, 4.3

Students will hear about the rise of AI in SE, how it is no longer a valid thought that these attacks tend to have poor grammar and if they can trust what they see. They will learn that because technology has become more secure, SE has become a more sophisticated method of attack with attackers using methods to bypass MFA (e.g. DUO), to prey on the good will of people, manipulating search engine results to place malicious links at the top of a user's search, and even using Internet of Things (IOT) devices such as refrigerators, vacuums, and wearables in their methods of attack. They will learn what can be done about these to defend themselves into the developing future.

Week 13: 2 Days
Bringing it all together and where to go from here

Assignment:

- **Reflection #4: Final thoughts of what they have learned and how they will change their behavior**

Assignment Due:

- Peer review of 2 team's presentations
- Weeks 9-12 Comprehension Essay Assignment: Understanding of instruction and assigned reading

Theme Integration: ELO1.1, 1.2, 2.1, 2.2, 3.1, 3.2, 4.1, 4.2, 4.3

Open discussion about what they have learned. How they felt about their presentation. What they have done, or plan to do, to improve their security, how they have, or will, reached out to family and friends to educate them about the severity of this risk. How well they feel organizations, social media platforms, and government is helping with the problem and what should they be doing. Students discussing will spark the discussion for other students. In the prior weeks of the course the instructor will simulate phishing attempts using physical and electronic mediums and reveal them during the classes of this week. Another open discussion topic in this week will be to talk about why people fell for them, or did not, and what they should do when they see one. Finally ending with an open conversation about how they feel this impacts what they have learned in other classes and how they will change their approach for their future classes.

Week 14: 1 Day
Final Study

Assignment:

- None

Assignments Due:

- Reflection #4: Final thoughts of what they have learned and how they will change their behavior

Academic Misconduct

Academic integrity is essential to maintaining an environment that fosters excellence in teaching, research, and other educational and scholarly activities. Thus, The Ohio State University and the Committee on Academic Misconduct (COAM) expect that all students have read and understand the University's Code of Student Conduct, and that all students will complete all academic and scholarly assignments with fairness and honesty. Students must recognize that failure to follow the rules and guidelines established in the University's Code of Student Conduct and this syllabus may constitute Academic Misconduct.

The Ohio State University's Code of Student Conduct (Section 3335-23-04) defines academic misconduct as: Any activity that tends to compromise the academic integrity of the University or subvert the educational process. Examples of academic misconduct include (but are not limited to) plagiarism, collusion (unauthorized collaboration), copying the work of another student, and possession of unauthorized materials during an examination. Ignorance of the University's Code of Student Conduct is never considered an excuse for academic misconduct, so I recommend that you review the Code of Student Conduct and, specifically, the sections dealing with academic misconduct.

If I suspect that a student has committed academic misconduct in this course, I am obligated by University Rules to report my suspicions to the Committee on Academic Misconduct. If COAM determines that you have violated the University's Code of Student Conduct (i.e., committed academic misconduct), the sanctions for the misconduct could include a failing grade in this course and suspension or dismissal from the University.

If you have any questions about the above policy or what constitutes academic misconduct in this course, please contact me.

Artificial Intelligence and Academic Integrity

There has been a significant increase in the popularity and availability of a variety of generative artificial intelligence (AI) tools, including ChatGPT, Sudowrite and others. These tools will help shape the future of work, research and technology but when used in the wrong way, they can stand in conflict with academic integrity at Ohio State.

All students have important obligations under the Code of Student Conduct to complete all academic and scholarly activities with fairness and honesty. Our professional students also have the responsibility to uphold the professional and ethical standards found in their respective academic honor codes. Specifically, students are not to use unauthorized assistance in the laboratory, on field work, in scholarship or on a course assignment unless such assistance has been authorized specifically by the course instructor. In addition, students are not to submit their work without acknowledging any word-for-word use and/or paraphrasing of writing, ideas or other work that is not your own. These requirements apply to all students undergraduate, graduate, and professional.

To maintain a culture of integrity and respect, these generative AI tools should not be used in the completion of course assignments unless an instructor for a given course specifically authorizes their use. Some instructors may approve of using generative AI tools in the academic setting for specific goals. However, these tools should be used only with the explicit and clear permission of each individual instructor, and then only in the ways allowed by the instructor.

Mental Health

As a student you may experience a range of issues that can cause barriers to learning, such as strained relationships, increased anxiety, alcohol/drug problems, feeling down, difficulty concentrating and/or lack of motivation. These mental health concerns or stressful events may lead to diminished academic performance or reduce a student's ability to participate in daily activities. The Ohio State University offers services to assist you with addressing these and other concerns you may be experiencing.

If you or someone you know are suffering from any of the aforementioned conditions, you can learn more about the broad range of confidential mental health services available on campus via the Office of Student Life's Counseling and Consultation Service (CCS) by visiting ccs.osu.edu or calling 614-292-5766. CCS is located on the 4th floor of the Younkin Success Center and 10th floor of Lincoln Tower. You can reach an on-call counselor when CCS is closed at 614-292-5766 and 24-hour emergency help is also available through the 24/7 by dialing 988 to reach the Suicide and Crisis Lifeline.

Sexual Misconduct

The Ohio State University is committed to building and maintaining a community to reflect diversity and to improve opportunities for all. All Buckeyes have the right to be free from harassment, discrimination, and sexual misconduct. Ohio State does not discriminate on the basis of age, ancestry, color, disability, ethnicity, gender, gender identity or expression, genetic information, HIV/AIDS status, military status, national origin, pregnancy (childbirth, false pregnancy, termination of pregnancy, or recovery therefrom), race, religion, sex, sexual orientation, or protected veteran status, or any other bases under the law, in its activities, academic programs, admission, and employment. Members of the university community also have the right to be free from all forms of sexual misconduct: sexual harassment, sexual assault, relationship violence, stalking, and sexual exploitation.

To report harassment, discrimination, sexual misconduct, or retaliation and/or seek confidential and non-confidential resources and supportive measures, contact the Civil Rights Compliance Office:

Online reporting form at http://civilrights.osu.edu/,
Call 614-247-5838 or TTY 614-688-8605,
Or Email equity@osu.edu

The university is committed to stopping sexual misconduct, preventing its recurrence, eliminating any hostile environment, and remedying its discriminatory effects. All university employees have reporting responsibilities to the Civil Rights Compliance Office to ensure the university can take appropriate action:

- All university employees, except those exempted by legal privilege of confidentiality or expressly identified as a confidential reporter, have an obligation to report incidents of sexual assault immediately.

- The following employees have an obligation to report all other forms of sexual misconduct as soon as practicable but at most within five workdays of becoming aware of such information: 1. Any human resource professional (HRP); 2. Anyone who supervises faculty, staff, students, or volunteers; 3. Chair/director; and 4. Faculty member.

Campus Free Speech Policy

Our shared values include a commitment to diversity and innovation. Pursuant to these values, the university promotes a culture of welcoming differences, making connections among people and ideas, and encouraging open-minded exploration, risk-taking, and freedom of expression. As a land-grant institution, the university takes seriously its role in promoting and supporting public discourse. To that end, Ohio State is steadfastly committed to protecting the First Amendment right to free speech and

academic freedom on its campuses, and to upholding the university's academic motto — "Education for Citizenship."

Title IX

Title IX makes it clear that violence and harassment based on sex and gender are Civil Rights offenses subject to the same kinds of accountability and the same kinds of support applied to offenses against other protected categories (e.g., race). If you or someone you know has been sexually harassed or assaulted, you may find the appropriate resources at http://titleix.osu.edu/ or by contacting the Ohio State Title IX Coordinator at titleix@osu.edu

Diversity

The Ohio State University affirms the importance and value of diversity in the student body. Our programs and curricula reflect our multicultural society and global economy and seek to provide opportunities for students to learn more about persons who are different from them. We are committed to maintaining a community that recognizes and values the inherent worth and dignity of every person; fosters sensitivity, understanding, and mutual respect among each member of our community; and encourages each individual to strive to reach his or her own potential. Discrimination against any individual based upon protected status, which is defined as age, color, disability, gender identity or expression, national origin, race, religion, sex, sexual orientation, or veteran status, is prohibited.

Religious Accommodations

Ohio State has had a longstanding practice of making reasonable academic accommodations for students' religious beliefs and practices in accordance with applicable law. In 2023, Ohio State updated its practice to align with new state legislation. Under this new provision, students must be in early communication with their instructors regarding any known accommodation requests for religious beliefs and practices, providing notice of specific dates for which they request alternative accommodations within 14 days after the first instructional day of the course. Instructors in turn shall not question the sincerity of a student's religious or spiritual belief system in reviewing such requests and shall keep requests for accommodations confidential.

With sufficient notice, instructors will provide students with reasonable alternative accommodations with regard to examinations and other academic requirements with respect to students' sincerely held religious beliefs and practices by allowing up to three absences each semester for the student to attend or participate in religious activities. Examples of religious accommodations can include, but are not limited to, rescheduling an exam, altering the time of a student's presentation, allowing make-up assignments to substitute for missed class work, or flexibility in due dates or research responsibilities. If concerns arise about a requested accommodation, instructors are to consult their tenure initiating unit head for assistance.

A student's request for time off shall be provided if the student's sincerely held religious belief or practice severely affects the student's ability to take an exam or meet an academic requirement and the student has notified their instructor, in writing during the first 14 days after the course begins, of the date of each absence. Although students are required to provide notice within the first 14 days after a course begins, instructors are strongly encouraged to work with the student to provide a reasonable accommodation if a request is made outside the notice period. A student may not be penalized for an absence approved under this policy.

If students have questions or disputes related to academic accommodations, they should contact their course instructor, and then their department or college office. For questions or to report discrimination or harassment based on religion, individuals should contact the Office of Institutional Equity.
(Policy: Religious Holidays, Holy Days and Observances)

Disability Services

The university strives to maintain a healthy and accessible environment to support student learning in and out of the classroom. If you anticipate or experience academic barriers based on your disability (including mental health, chronic, or temporary medical conditions), please let me know immediately so that we can privately discuss options. To establish reasonable accommodations, I may request that you register with Student Life Disability Services. After registration, make arrangements with me as soon as possible to discuss your accommodations so that they may be implemented in a timely fashion.

If you are ill and need to miss class, including if you are staying home and away from others while experiencing symptoms of viral infection or fever, please let me know immediately. In cases where illness interacts with an underlying medical condition, please consult with Student Life Disability Services to request reasonable accommodations. You can connect with them at slds@osu.edu; 614-292-3307; or slds.osu.edu.

THE OHIO STATE UNIVERSITY

CybrSec 2111– Social Engineering: Spams, Scams, and Saving Your Assets

Course Schedule

Week 1: Introductions, About the class and assignments, and how to succeed. Basics of Information Security

Preread Syllabus and Carmen Modules
Assignment: Partners for presentations
Assignment due: None

Week 2: Social Engineering Introduction

Preread
https://www.sciencedirect.com/science/article/pii/S2451958821000749
Chapters 1, 2, 6 https://www.mitnicksecurity.com/the-history-of-social-engineering
Assignment: None
Assignment due: None

Week 3: Psychology of Deception and the Ethics of Social Engineering

Preread
https://www.mdpi.com/1677374
https://www.mitnicksecurity.com/blog/ways-hackers-use-social-engineering-to-trick-your-employees
https://www.social-engineer.org/social-engineering/amygdala-hijacking-and-social-engineering/
https://ojs.victoria.ac.nz/wfeess/article/view/7671/6807
Assignment: Team outline of presentation: Social Engineering – What is it and How Can I Protect Myself? (Demographic audience)
Assignment due: Partners for presentations (otherwise randomly assigned)
Quiz #1

Week 4: Demographic Worldview

Preread
https://www.ncbi.nlm.nih.gov/books/NBK589697/
https://kirwaninstitute.osu.edu/implicit-bias-module-series
https://www.pageon.ai/blog/how-to-present-visual-presentations-to-older-adults
Assignments: Reflection #1: Your Implicit Bias results.
Assignment due: none

Week 5: Common Social Engineering Tactics

Preread Chapter 3: https://www.mitnicksecurity.com/the-history-of-social-engineering
Assignment: None
Assignment due: Reflection #1: Your Implicit Bias results
Quiz #2

Week 6: Recognizing and Avoiding Scams

Preread Chapter 4: https://www.mitnicksecurity.com/the-history-of-social-engineering
Assignment: Reflection #2: Student vulnerability to Social Engineering
Assignments due: Team outline of their presentation

Week 7: Protecting Your Digital Footprint

Preread https://www.identityguard.com/news/how-to-protect-your-digital-footprint
Assignment: Reflection #3: Visit assigned demographic location for discussion and
Assignments due: Reflection #2: Student Vulnerability to Social Engineering

Quiz #3

Week 8: Major social engineering events what could have been done

Assignment: 15 minute recorded video: Team presentations Social Engineering – What is it and How Can I Protect Myself? (demographic as planned audience)
Assignment due: None

Week 9: Social Engineering in Social Media and the workplace

Preread Chapter 5 and 7: https://www.mitnicksecurity.com/the-history-of-social-engineering
Assignment: None
Assignment due: Reflection #3: How is the demographic targeted and what can they do to protect themselves

Week 10: Emerging Threats

Guest Speaker: Cybersecurity Expert

Preread https://abnormalsecurity.com/blog/soc-expert-perspectives-social-engineering-threats
Assignment: Peer review of 2 teams' videos
Assignment Due: 15 minute recorded video

Quiz #4

Week 11: Bringing it all together

Preread: Designing an effective presentation - https://journals.plos.org/ploscompbiol/article?id=10.1371/journal.pcbi.1009554
How they felt about their first pass at the presentation
The rules of engagement for the focus group
Assignment: Prepare for the demographic focus group
Assignment Due: Peer review of 2 team's presentations

Week 12: Tuning the Presentation

Preread: comments from peer reviews and instructor
Recap how to build an effective presentation for the demographic
In-class work on their presentation.
Assignment: Update presentation.
Assignment Due: None

Week 13: Refining the Presentation

In class work on their presentation.
Assignments:
    Updates to Presentation
Assignments Due: Presenting to the demographic focus group

Week 14-15: Finalizing the Presentation

Assignment: Finalizing the Presentation based on discussion and focus group feedback
Assignments Due: Demographic Presentation at faculty arranged location

GE Theme course submission worksheet: Lived Environments

Overview

Courses in the GE Themes aim to provide students with opportunities to explore big picture ideas and problems within the specific practice and expertise of a discipline or department. Although many Theme courses serve within disciplinary majors or minors, by requesting inclusion in the General Education, programs are committing to the incorporation of the goals of the focal theme and the success and participation of students from outside of their program.

Each category of the GE has specific learning goals and Expected Learning Outcomes (ELOs) that connect to the big picture goals of the program. ELOs describe the knowledge or skills students should have by the end of the course. Courses in the GE Themes must meet the ELOs common for **all** GE Themes and those specific to the Theme, in addition to any ELOs the instructor has developed specific to that course. All courses in the GE must indicate that they are part of the GE and include the Goals and ELOs of their GE category on their syllabus.

The prompts in this form elicit information about how this course meets the expectations of the GE Themes. The form will be reviewed by a group of content experts (the Theme Advisory) and by a group of curriculum experts (the Theme Panel), with the latter having responsibility for the ELOs and Goals common to all themes (those things that make a course appropriate for the GE Themes) and the former having responsibility for the ELOs and Goals specific to the topic of **this** Theme.

Briefly describe how this course connects to or exemplifies the concept of this Theme (Lived Environments)

In a sentence or two, explain how this class "fits' within the focal Theme. This will help reviewers understand the intended frame of reference for the course-specific activities described below.

Although not the traditional lived environment, cyberspace is a lived environment that unites humans and technologies and this course, Social Engineering: Spams, Scams, and Saving Your Assets, teaches students about the tactics and techniques hackers use to manipulate people in their on-line world to make errors which result in significant losses and stress. Social Engineering lived environments have dynamic demographics based on work, social, age, sex, culture, and even relationship status and and individuals may defend well in platforms like Carmen and Email, but may be more susceptible in their Social Media lived environment due to perceived peer pressure or fear of missing out (FOMO).

Connect this course to the Goals and ELOs shared by *all* Themes

Below are the Goals and ELOs common to all Themes. In the accompanying table, for each ELO, describe the activities (discussions, readings, lectures, assignments) that provide opportunities for students to achieve those outcomes. The answer should be concise and use language accessible to colleagues outside of the submitting department or discipline. The specifics of the activities matter—listing "readings" without a reference to the topic of those readings will not allow the reviewers to understand how the ELO will be met. However, the panel evaluating the fit of the course to the Theme will review this form in conjunction with the syllabus, so if readings, lecture/discussion topics, or other specifics are provided on the syllabus, it is not necessary to reiterate them within this form. The ELOs are expected to vary in their "coverage" in terms of number of activities or emphasis within the course. Examples from successful courses are shared on the next page.

Goal 1: Successful students will analyze an important topic or idea at a more advanced and in-depth level than the foundations. In this context, "advanced" refers to courses that are e.g., synthetic, rely on research or cutting-edge findings, or deeply engage with the subject matter, among other possibilities.

Goal 2: Successful students will integrate approaches to the theme by making connections to out-of-classroom experiences with academic knowledge or across disciplines and/or to work they have done in previous classes and that they anticipate doing in future.

	Course activities and assignments to meet these ELOs
ELO 1.1 Engage in critical and logical thinking.	Today's student reside as much in the online environment as they do in their physical environment. They are subject to many threats and this course will provide the students the understanding of social engineering, and the methodology and psychology of it. Students will hear from cybersecurity, psychology, and demographic experts to help them understand the threat for themselves and for others. They will learn how targeted populations are manipulated and what they can do. Through this education, they will develop critical and logical thinking of how to discern social engineering attacks and protect themselves. By the end of this course they will be able to recognize tactics of social engineers, and not only how they should respond to these attacks to protect themselves, but also how they can teach others to do the same.
ELO 1.2 Engage in an advanced, in-depth, scholarly exploration of the topic or ideas within this theme.	Through the reading, exercises, and instruction, students will have a good understanding of the threat of social engineers and will be able to apply this understanding of how they and others are manipulated within their online environment. Through reflection assignments, students will identify their own susceptibility to being manipulated and their vulnerability to social engineering and will examine the consequences on their information and through the essay assignments (formerly quizzes) they will contemplate and demonstrate their understanding of the assigned readings and instruction. They will use what they have learned in class and work in a 3-4 person team of students develop a persuasive presentation.
ELO 2.1 Identify, describe, and synthesize approaches or experiences.	<u>Lecture</u> Course materials support the learning of basic cybersecurity and psychology concepts relevant to social engineering and their online presence, including: • Tactics of a social engineer • How to recognize and avoid scams. • How to protect their digital footprint. • Social Engineering in social media, the workplace, and other sources. • How to coach others about identifying potential threats. <u>Reading</u> All material used for this class is freely available. Each module provides important reading material to expose students to concepts prior to the instruction and set the basis of learning of the topic. <u>Reflections</u> Students will reflect upon: • Their implicit bias: Students will learn about the psychology of social engineering and how about their own implicit bias toward

	the specific demographic and how those biases can be used in social engineering attacks. Students will reflect how this made them understand their implicit bias and what they can do about it. • How an assigned demographic is, and feels targeted. • Their own Vulnerabilities to social engineering: Students will learn methods of social engineering attacks and will identify their own vulnerabilities to social engineering. • Final thoughts of what they have learned and what they will change <u>Knowledge checks and assessments</u> At the end of each class will be knowledge checks performed in TopHat. These knowledge checks are not graded but will identify where students may not understand the content and to encourage additional conversation. Each module builds upon understanding of prior course topics, so Comprehension Essay Assignments are used to evaluate understanding of material and concepts.
ELO 2.2 Demonstrate a developing sense of self as a learner through reflection, self-assessment, and creative work, building on prior experiences to respond to new and challenging contexts.	Students will have multiple activities to develop their sense of self through this course. Assignments are intentionally scaffolded to help students understand more as the course continue – not only of the content, but also of their perceptions. Open discussions in class will also allow open reflection. Students will work in a team to build their persuasive presentation which they will receive feedback from other students.

Goals and ELOs unique to Lived Environments

Below are the Goals and ELOs specific to this Theme. As above, in the accompanying Table, for each ELO, describe the activities (discussions, readings, lectures, assignments) that provide opportunities for students to achieve those outcomes. The answer should be concise and use language accessible to colleagues outside of the submitting department or discipline. The ELOs are expected to vary in their "coverage" in terms of number of activities or emphasis within the course. Examples from successful courses are shared on the next page.

GOAL 3: Successful students will explore a range of perspectives on the interactions and impacts between humans and one or more types of environment (e.g. agricultural, built, cultural, economic, intellectual, natural) in which humans live.

GOAL 4: Successful students will analyze a variety of perceptions, representations and/or discourses about environments and humans within them.

	Course activities and assignments to meet these ELOs
ELO 3.1 Engage with the complexity and uncertainty of human- environment interactions.	The topic of social engineering is fraught with complexity and uncertainty of human-environment interaction. Social Engineering is the soft-underbelly of the hardened shell of cybersecurity. Throughout this course, students will hear about the psychology, demographics, and cybersecurity integration of Social Engineering which will expose the students to the mindset of hackers and how people are manipulated in the cyber lived environment. Students will be assigned to talk to a member of the assigned demographic that additional information will aid to develop and deliver a persuasive presentation. Four assignments will lead students to research and consider this topic:

	1) Student's vulnerability to social engineering, 2) Students implicit bias to the demographic, 3) How the demographic is, and feels, targeted 4) Final thoughts of what they have learned and how they will change
ELO 3.2 Describe examples of human interaction with and impact on environmental change and transformation over time and across space.	Students will learn about how humans interact with the cyber environment by hearing examples of social engineering attacks. They will hear the history of social engineering attack in the early days of individual, less sophisticated attacks to the complicated and enterprise-developed turn-key social engineering attacks available for hire and now the developing use of AI for attacks. They will learn the importance of education and how it can change the outcome to protect this soft under-belly. Through this course students will lower their risk and their future employers as they will have better security awareness. They will have the knowledge to become change agents for their in-real-life (IRL) friends, family, business, classmates, and colleagues.
ELO 4.1 Analyze how humans' interactions with their environments shape or have shaped attitudes, beliefs, values and behaviors.	Students will read, learn, and discuss attack methods and their growing sophistication. Students will reflect on these and use their growing knowledge to determine methodology to mitigate the risks.
ELO 4.2 Describe how humans perceive and represent the environments with which they interact.	Students will learn that the perception of the online world varies across the demographics, but there is a recurring theme: People are skeptical to believe many sources in today's world. Hackers know a well-crafted phish which targets their income, life, or family and people are willing to believe anything. Students will learn the more educated people become the more likely they will be able to recognize and avoid the attack and they will learn how to be the change agents in their different lived environments.
ELO 4.3 Analyze and critique conventions, theories, and ideologies that influence discourses around environments.	In this course students will learn more about their own lived environment and how their own actions may make them more and others vulnerable. Students will hear about tactics, information, and disinformation which contribute to fear, uncertainty, and doubt. These result in reactive and possibly detrimental actions. Education is the solution and by completing this course students will be better equipped to identify and protect themselves against attacks and will be able to educate others to do the same.