WILMINGTON UNIVERSITY
COLLEGE OF TECHNOLOGY
BASIC COURSE INFORMATION

COURSE TITLE: Psychology of a Cyber Attacker

COURSE NUMBER: SEC305

I. MAJOR INSTRUCTIONAL OBJECTIVES:

Objective A: Explore the fundamentals of social engineering.
A-1: Explain what a Cyber Attack is/is not
A-2: Explore the history and categories of social engineers
A-3: Explain ethical responsibilities of social engineers
A-4: Describe active/passive information gathering

Objective B: Identify the methodology, tactics and motivation of social engineering
B-1: Explain how to gather information from various sources
B-2: Describe the inter-relationships among public information.
B-3: Identify motivating factors.
B-4: Describe common attacks and real world examples.

Objective C: Fine tune social engineering execution and identification
C-1: Identify successful cues, rapport, and microexpressions
C-2: Identify threats such as Insider Threat, Inadvertent Disclosures and Advanced Persistent Threat
C-3: Explain defense and prevention / security awareness

Objective D: Execute the tools and techniques of social engineering
D-1: Define the goals of reporting, including content
D-2: Review the real world needs of social engineers, and skillsets required
D-3: Review supplemental education options to continue social engineer career path
D-4: Submit hands-on social engineering passive reconnaissance testing
D-5: Leverage passive results to execute active testing on fictitious target

II. CLASS PARTICIPATION:

Students are expected to attend class and participate actively and in a positive way. Questions and relevant observations are encouraged and enrich the experience of the entire class. Computers in the classrooms are intended to be used as tools to enhance the students' learning experience. Instant messaging, gaming, emailing, and surfing the web are distractions to the student, the surrounding students, and the instructor and constitute inappropriate behavior. Students are ethically obliged to avoid these and similar practices.