# Cybersecurity and Human Behavior (CYHB)

Course information contained within the Bulletin is accurate at the time of publication in July 2024 but is subject to change. For the most up-to-date course information, please refer to the Course Catalog.

**CYHB 2001. Introduction to Cybersecurity. 3 Credit Hours.**
This course will equip students with a foundational understanding of cybersecurity and expose them to various cybersecurity topics, such as cyber threat intelligence, digital forensics, Open Source Intelligence (OSINT) investigations and analysis, social engineering and penetration testing, and governance, risk, and compliance.

**Repeatability:** This course may not be repeated for additional credits.

**CYHB 3001. Social Engineering and Cybersecurity. 3 Credit Hours.**
Social engineering (SE) is a technique where psychological persuasion of humans is used to conduct reconnaissance (identify systems operating at target facilities), obtain information intended to secure electronic systems (passwords), or to encourage targets to inadvertently provide access to electronic systems and information (downloading and executing malicious files) that are disguised as familiar or benign. The average organization is targeted by over 700 SE attacks each year. This course will equip students with a foundational understanding of SE and expose them to various aspects of SE, such as OSINT, phishing, vishing, elicitation, pretexting, and psychological persuasion.

**Repeatability:** This course may not be repeated for additional credits.

**Pre-requisites:** Minimum grade of C- in CYHB 2001 and PHIL 3228.

**CYHB 3002. Cybersecurity, Surveillance and Privacy. 3 Credit Hours.**
We live in an era of 24-7 surveillance where, every day, transactions engaged in by individuals generate ever expanding amounts of personal information, including credit card and bank transactions, purchasing histories, location tracking, health information, and information shared on social media. The acquisition, management, analysis, dissemination, and security of these data raise increasingly important issues as they reside on servers and storage media where they can be accessible to commercial enterprises, government agencies, and malicious actors. Students in this class will learn about the evolution and different types of surveillance, the intersection between surveillance, privacy, and cybersecurity, and specific instances of surveillance (e.g., health and the body, workplace and education, underrepresented communities and individuals, capitalism, and online/internet-based monitoring).

**Repeatability:** This course may not be repeated for additional credits.

**Pre-requisites:** Minimum grade of C- in CYHB 2001 and PHIL 3228.

**CYHB 3085. Internship in Cybersecurity and Human Behavior. 3 Credit Hours.**
Internship with law enforcement and other related agencies, rehabilitation and prevention programs, corporations, and other organizations working on issues of cybersecurity. In this experience, students identify potential career interests, synthesize prior knowledge from the classroom with direct experience, critically examine the criminal justice system in operation, and sharpen analytical and observational skills. This course requires 150 hours of work at a placement site. NOTE: Enrollment requires permission from the instructor. Open to students with 60 or more credits with a declared major, minor, or certificate program in Cybersecurity and Human Behavior. This course may be taken one time to fulfill an elective in the major, minor, or certificate program in Cybersecurity and Human Behavior.

**Field of Study Restrictions:** Must be enrolled in one of the following Fields of study: Cybersec + Human Behavior.
**Class Restrictions:** Must be enrolled in one of the following Classes: Junior 60 to 89 Credits, Senior 90 to 119 Credits, Senior/Fifth Year 120+ Credits.

**Repeatability:** This course may not be repeated for additional credits.

**CYHB 3096. Cybersecurity Governance, Risk, Compliance and Policy. 3 Credit Hours.**
Students in this class will learn about cybersecurity governance, risk management, risk and controls, incident response to cyberattacks and their costs and harms, cybersecurity compliance, introduction to various technical and industry frameworks (ISO 27000/1, NIST 800-53, MITRE ATT&CK) and how to map these frameworks effectively, and developing cybersecurity policies that are informed by these frameworks. Students will go through a GRC assessment and audit process for a mock organization.

**Course Attributes:** WI

**Repeatability:** This course may not be repeated for additional credits.

**Pre-requisites:** Minimum grade of C- in CYHB 2001 and PHIL 3228.

**CYHB 4001. Community Engagement and Cyber Hygiene. 3 Credit Hours.**
Cyber hygiene refers to the practices and steps that individuals and organizations take to maintain system health and improve online security of their computers or other digital devices. This course provides students with an experiential learning opportunity by applying various cybersecurity and digital hygiene concepts and principles to real-world settings. Specifically, students will engage with various organizations in North Philadelphia to provide an assortment of services such as training and awareness and cyber clinics. Students in this class will learn about topics such as digital literacy, cyber hygiene, community outreach and engagement, cyber hygiene practices for personal devices, home, and remote working and learning, and principles of community engagement.

**Repeatability:** This course may not be repeated for additional credits.

**Pre-requisites:** Minimum grade of C- in CYHB 2001, CYHB 3001, and PHIL 3228.