Unit 1: Introduction to Security

Content Area: **Business**
Course(s): **Generic Course**
Time Period: **Semester 1**
Length: **3 weeks**
Status: **Published**

Enduring Understandings

EU 1.1: The Human Factor in Security
People are often the most versatile and frequently targeted entry point in a system's security perimeter. Technically sound systems can be entirely bypassed when adversaries successfully exploit predictable human emotions—like urgency and fear—across various communication channels to manipulate victims into volunteering access, sharing data, or executing malicious code.

EU 1.2: Cryptographic and Policy Defenses of Access Control
Authentication security relies on mathematical complexity and modern defensive architecture, not user compliance. Because human behavior resists strict complexity rules and frequent changes, securing access requires cryptographic safeguards (like one-way hashing and salting) and modern, evidence-based password frameworks (such as NIST guidelines) that drastically increase the computational cost of a breach for an attacker.

EU 1.3: Shared Medium Vulnerabilities
The open, broadcast nature of wireless networks inherently compromises physical security boundaries and requires active, end-to-end encryption. Because radio frequencies can be intercepted, spoofed, or disrupted by adversaries of varying skill levels, defenders must operate under a zero-trust model on public networks, using tactical individual defenses (like VPNs) to protect data confidentiality and integrity.

EU 1.4: The Mechanization of Adversarial Tactics via AI
Artificial intelligence removes the traditional bottlenecks of scale, language barriers, and signature predictability for malicious actors. By leveraging generative models, automated mutation, and prompt manipulation, adversaries can execute highly personalized, sophisticated, and structurally evasive attacks at a volume and speed that legacy, static defense systems are fundamentally unequipped to handle.

EU 1.5: Augmentation and Oversight in Modern Defense
Modern cyber defense is an asymmetric data problem that requires AI for operational scale, paired with human oversight for strategic accuracy. While machine learning is mandatory to ingest, correlate, and baseline millions of daily security events, the persistent threats of false metrics, adversarial manipulation, and an ongoing "AI-vs-AI arms race" mean that automated tools must augment—rather than replace—human risk analysis and decision-making.

Standards

CS.9-12.8.1.12.IC.1	Evaluate the ways computing impacts personal, ethical, social, economic, and cultural practices.
CS.9-12.8.1.12.IC.3	Predict the potential impacts and implications of emerging technologies on larger social, economic, and political structures, using evidence from credible sources.
CS.9-12.8.1.12.NI.2	Evaluate security measures to address various common security threats.
CS.9-12.8.1.12.NI.3	Explain how the needs of users and the sensitivity of data determine the level of security implemented.
CS.9-12.8.1.12.NI.4	Explain how decisions on methods to protect data are influenced by whether the data is at rest, in transit, or in use.

Essential Questions

Topic 1.1: Understanding Social Engineering

How do adversaries use specific delivery channels and psychological tactics (urgency and intimidation) to manipulate human behavior, and what are the resulting impacts on security?

Topic 1.2: Suspicious Website Logins

How do the distinct mechanisms of credential attacks mathematically and cryptographically expose the flaws of legacy password policies, and how do modern controls like salting and NIST guidelines neutralize them?

Topic 1.3: Best Practices for Public Networks

How do wireless attacks (evil twins, jamming, and war driving) threaten the CIA triad based on an adversary's skill level, and how effectively do standard individual defenses mitigate these risks?

Topic 1.4: AI-Based Cybersecurity Attacks

How does generative AI fundamentally change the scale, quality, and detection-evasion capabilities of social engineering, malware, and prompt-based exploits?

Topic 1.5: Leveraging AI in Cyber Defense

Why does the scale of modern security data necessitate an AI-driven approach to threat detection and mitigation, and why must human oversight remain a critical counterweight in the AI-vs-AI arms race?

Knowledge and Skills

Topic 1.1: Understanding Social Engineering:

- Identify social engineering attack types by delivery channel (phishing/email. vishing/voice, smishing/text, in-person)
- Explain the two CED-named psychological tactics - intimidation and urgency - and how each drives action without thinking
- Describe the three victim impact categories: revealing personal info, revealing secure info (OTP/codes), downloading malware
- Distinguish phishing (mass) from spear phishing (targeted/personalized) on the same email channel
- Analyze a scenario to identify the attack type and psychological principle being exploited

Topic 1.2: Password Attacks and Authentication:

- Identify all three CED signs of an online password attack: many failed attempts in short duration, login at unusual times, login from unknown devices
- Explain the three common password patterns adversaries exploit and how a targeted dictionary is constructed
- Apply the three defenses: long/random/unique passwords or passphrases, avoiding personally meaningful words, enabling MFA
- Distinguish a targeted dictionary attack from a generic brute-force attack
- Recognize that MFA is the highest-value individual defense against password compromise

Topic 1.3: The Dangers of Public Wi-Fi:

- Identify the type of adversary conducting a cyberattack, distinguishing between low-skilled and high-skilled adversaries
- Recognize that adversaries have a variety of motivations, including greed, desire for recognition, dedication to a cause, revenge, politics, or beliefs
- Identify all three CED types of wireless attacks: evil twin, jamming, and war driving
- Explain how individuals can protect themselves from some cyberattacks: verify network name before joining, avoid joining unprotected wireless networks, consider using a VPN
- Analyze a scenario to consider the consequences of joining an unprotected wireless network

Topic 1.4: AI-Augmented Cyberattacks:

- Identify all six ways adversaries use AI: deepfakes, AI phishing in any language, prompt injection, data poisoning, AI reconnaissance, AI malware writing
- Recognize that AI removes the "unnatural language" detection cue previously used to identify phishing
- Explain four individual defenses: shared secrets, MFA, not entering personal data into AI tools, verifying AI output against non-AI sources
- Understand why voice-based authentication is increasingly at risk as AI deepfake capabilities grow
- Apply the correct CED defense to a specific AI attack type in a scenario

Topic 1.5: AI for Cyber Defense:

- Explain three ways AI assists defenders: reviewing security configs, analyzing code for vulnerabilities, suggesting detection rules -- all require human review
- Explain why AI is necessary for threat detection: millions of daily network events exceed human capacity to examine
- Describe how AI sorts malicious from harmless events, then alerts humans or takes corrective action

- Apply the human-in-the-loop principle: all three 1.5A areas require qualified human review before implementation
- Distinguish 1.4 (AI used to attack) from 1.5 (AI used to defend)

Transfer Goals

Students will be able to immediately recognize and stop social engineering attacks by spotting psychological triggers like rush tactics or fear before reacting.

Students will be able to secure their online accounts by using strong passphrases and password managers rather than relying on weak, easily guessed passwords.

Students will be able to safely navigate public networks by automatically using tools like VPNs to stop hackers from spying on their data.

Students will be able to utilize AI tools for cybersecurity while remaining skeptical enough to double-check the AI's work for mistakes or biases.

Resources

AP Cybersecurity Course and Exam Description, Effective Fall 2026, College Board

AP Cybersecurity Course Framework, Effective 2026-2027 School Year, College Board

AP Cybersecurity Curriculum, by APCSExamPrep.com

Cybersecurity Curriculum Materials, by Cyber.org

Cyber Range, provided by Cyber.org