Why Cybersecurity Education Should Be Required in Every High School

Format: 5-Paragraph Argumentative | Level: High School | ~600 words

Every student who graduates high school knowing how to analyze a primary source but not how to identify a phishing email has received an education that does not match the environment they are entering. Cybersecurity literacy, the ability to recognize social engineering, manage credentials securely, and understand basic network behavior, has become as foundational as financial literacy for daily life in a connected world. Yet most high school curricula treat it as an elective or ignore it entirely. Cybersecurity education should be required at the secondary school level not because every student will enter the field, but because every student will be targeted by those who have.

The most common cyber threats facing individuals today do not require sophisticated technical knowledge to execute. Phishing attacks, credential stuffing, and social engineering succeed because their targets lack the baseline awareness to recognize them. A 2023 report from the Cybersecurity and Infrastructure Security Agency found that 80 percent of data breaches involved stolen or weak credentials, a problem that basic password hygiene education could meaningfully reduce. These are not technical failures; they are literacy failures, and schools are in the best position to address them before students enter adult digital life.

A second reason for requiring cybersecurity education is the significant and growing gap between workforce demand and supply of qualified practitioners. The global shortage of cybersecurity professionals was estimated at 3.4 million in 2022. That gap cannot be closed by university programs alone, particularly when students arrive at those programs with no prior exposure to the field. Secondary school courses in cybersecurity serve both as a pipeline for future professionals and as a filtering mechanism, identifying students with aptitude who might not have encountered it otherwise. Countries including Israel, Estonia, and the United Kingdom have incorporated cybersecurity education into their national curricula with measurable effects on both public awareness and professional development.

The most common objection to mandating cybersecurity education is that teachers are not equipped to deliver it. This is an implementation problem, not an argument against the policy. The same objection was raised against financial literacy requirements and computer science mandates, and both have been addressed through curriculum development, teacher training, and partnerships with industry and higher education. The College Board piloted an AP Cybersecurity curriculum in 2022 and expanded it nationally, providing a model that requires no prior teacher expertise and produces measurable student outcomes. The barrier is not the absence of workable models; it is the absence of

political will to require them.

Cybersecurity education is not a technical elective for students interested in computers. It is a civic necessity for students who will manage their financial accounts, health records, and communications through networked systems for the rest of their lives, and who will be targeted by criminal and state-sponsored actors who have made studying those systems their profession. Requiring it in every high school is not a burden on the curriculum. It is an overdue correction to a gap that costs individuals and institutions billions of dollars a year in entirely preventable losses.