

INTRO TO CYBERSECURITY

Ideal for learners who want to take their first step into cybersecurity, this introductory course aims to familiarize attendees with the industry, its key concepts, and commonly used tools. A real-world Olympics cyber-attack scenario leads the learning experience as participants dive into the world of cybersecurity and its impact. The course also discusses primary players in this space and their motivations, as well as highlights different roles in the field.

A fast-paced world demands self-paced classes, which is why our course enables your team to learn remotely, on their own schedule. Intro to Cybersecurity is an online, self-paced program that should take 30 hours to complete.

Overview

**FORMAT**

Online, Self-Paced

**DURATION**

30 Hours

**ACCESS**

Browser-Based

**PREREQUISITES**

None



Who Is This For?

- Cybersecurity newbies who need an introduction to the basics
- Professionals who need to be able to talk about basic security concepts, principles, and terms, but don't need to know the in-the-weeds details
- Managers who would like to better understand security fundamentals to help them make more informed decisions

Intro to Cybersecurity Course Structure

<p>MODULE 1</p> <p>The Cybersecurity World and Crime</p>	<ul style="list-style-type: none"> Gain an understanding of the need for cybersecurity in every organization. Grow comfortable with fundamental cybersecurity procedures. Uncover the most prevalent security threats.
<p>MODULE 2</p> <p>Attackers and APTs</p>	<ul style="list-style-type: none"> Study the various kinds of attackers, their motivations, and how they launch and distribute their objectives. Get insight into advanced persistent threats and the most well-known groups over the past few years. Understand the cyber kill chain and all the processes that attackers follow.
<p>MODULE 3</p> <p>Mitigating Risk and Taking Control</p>	<ul style="list-style-type: none"> Delve into the significance of ethical hacking. Discover how employee education, such as enforcing password policies, can prevent cyberattacks. Explore risk management processes, and the most well-known policies, procedures, standards, and guidelines, including PCI, PHI, and PII. Practice managing a risk process.

What's Included in the Course



HANDS-ON ACTIVITIES

Unique virtual labs and exercises are based on real-world scenarios, helping learners grasp new concepts quickly.



FLEXIBLE LEARNING

Learners go at their own pace within a supportive community environment that maximizes engagement.



STAYING AHEAD OF THE CURVE

We regularly update our curriculum to keep pace with the latest in cybersecurity, including AI and new technologies.

About C.A.R.E [Cyber Awareness and Response Education]

C.A.R.E empowers lifelong learners through specialized cybersecurity programs designed to upskill and reskill for today's digital landscape. In partnership with academic institutions, corporations, and government bodies across the globe, we deliver comprehensive training and advanced professional development.

Driven by a team of cybersecurity and technology experts, C.A.R.E blends the experience of seasoned educators, industry professionals, and cyber specialists—united in their mission to bridge the global cybersecurity skills and talent gap.

