

CompTIA CyberSecure™



Online security training for everyone!

CompTIA CyberSecure™ is a self-paced training course of security best practices vital for employees to protect your business.

The course focuses on implications of security behaviors of everyone in the workplace...not just the IT department. The 60-minute course covers online and offline behaviors that reduce security risks.

WHO SHOULD TAKE CompTIA CYBERSECURE?

CompTIA CyberSecure provides results-driven behavior modification training on information security for every member of an organization, from a project manager to a facilities maintenance engineer and even the CEO.

The training uses an innovative approach to content development to create this fun and interactive course. No more boring eLearning!

HOW WAS CompTIA CYBERSECURE DEVELOPED?

The objectives for CompTIA CyberSecure were developed and approved with the help of the CompTIA IT Security Community, a group of the industry's leaders in the IT security space.

No one is more qualified to serve the IT industry by educating end-users about these critical security issues than CompTIA, the voice of the IT industry and the leader in vendor-neutral IT certification.

Cybersecurity is for everyone... not just the IT department.

79% of companies believe cybersecurity threats are rising.

52% think the element of human error in security threats is increasing.

FIND OUT MORE

Look for more information on this exciting new product at CyberSecure.org

CompTIA CyberSecure Learning Objectives

Learning Objective 1: You are the Best Defense

Understand that the user can and should effectively protect him/herself and her company from information leaks.

- Understand that information security is the responsibility of every employee in an organization.
- Identify the human as the target of malicious actions, not technology.
- Understand that the user can make a difference.

Learning Objective 2: Overview of information security threats

Understand the basic categories of information security threats.

- Identify personally identifiable information.
- Understand that leaks can come from inside or outside of a network.
- Understand the way information can be compromised.

Learning Objective 3: Cultivating a Safe Mindset

Understand how to cultivate a safe information mindset.

- Understand the role of the IT and HR departments in regard to policy within info security.
- Understand healthy vigilance and skepticism.

Learning Objective 4: Cultivating a Safe Environment

Understand how to cultivate a safe environment.

- Understand how to cultivate a safe office.
- Understand how to cultivate a safe environment when working remotely.

Learning Objective 5: Staying Safe Online

Understand how to implement safety strategies online.

- Understand that practicing situational awareness, healthy vigilance, and skepticism will help keep the user as well as their data safe.



Top 5 Reasons human error leads to security incidents:

1. Increased use of social media by staff
2. Failure of staff to understand new threats
3. General negligence/carelessness towards security
4. Lack of security expertise with websites and applications
5. Failure of IT staff to follow security procedures and policies

**CompTIA
CyberSecure
can help!**

Visit [CyberSecure.org](https://www.comptia.org/cybersecure) for a free trial!

As a OneBeacon partner, CompTIA Cybersecure is available to OneBeacon insureds at a discounted rate of \$1.00 a seat. Contact Teresa Varela at tvarela@comptia.org or cybersecure-ops@comptia.org to start your purchase or with any questions.