Cybersecurity for Employees Working from Home
Course Instructions

Author: Robert Minniti

Copyright © 2021 CCH CPELink

Instructions to Participants

To assist the participant with navigating the learning process through to successful completion, this course has been produced with the following elements:

Overview of Topics / Table of Contents: In this electronic format you'll find a slide menu on the left side of the screen. This serves as your overview of topics for the program. You may navigate to any topic by clicking on the slide name.

Definition of Key Terms / Glossary: You'll find key terms defined for this program in the course information on the following page(s).

Index / Key Word Search: You can find information quickly in the PDF materials (slide handout plus any additional handouts) by using the search function built into your Adobe Reader.

Review Questions: Questions that test your understanding of the material are placed throughout the course. You'll see explanatory feedback pop up for each incorrect answer, and reinforcement feedback for the correct answer for every review question.

Final Exam: The final exam measures if you have gained the knowledge, skills, or abilities outlined in the learning objectives. You may submit your final exam at the end of the course. Exams are graded instantly. A minimum score of 70% is required to receive the certificate of completion. **You have one year from date of purchase to complete the course.**

Course Evaluation: Once you have successfully passed your online exam, please complete our online course evaluation. Your feedback helps Wolters Kluwer maintain its high quality standards!

About This Course

This section provides information that is important for understanding the course, such as course level and prerequisites. Please consider this information when filling out your evaluation after completing the course.

Publication Date: April 2021

Course Description
With the 2020 pandemic many organizations have employees working from home for the first time. This creates additional cyber security risks for the employees and their organizations.

This course is designed for employees who are working from home, who would like to obtain an understanding of data and cybersecurity. You have probably heard of some of the more common types of cyber crimes such as ransomware, spyware, computer viruses, phishing, vishing, spoofing, data breaches, denial of service attacks, hacking, etc.

This course is also designed to familiarize accounting, auditing, consulting, and tax professionals who are not information technology (IT) experts on data breach and cybersecurity risks and internal controls. We will cover the material in a plain language, nontechnical manner. We will cover what you need to know, but not how to write the computer programs or code.

Learning Objectives
Upon successful completion of this course, participants should be able to:
- Describe cybersecurity
- Identify various types of cyber fraud risks
- Recognize cybersecurity risk for an organization
- Recognize IT system cybersecurity risks
- Recognize how to prevent and detect cyber frauds
- Describe what would use facial recognition to log you onto a computer
- Identify how to anonymously surf the web
- Recognize what is used in conjunction with the COSO framework
- Describe where you would most likely find online banking websites

NASBA Field of Study
Information Technology. Some state boards may count credits under different categories—check with your state board for more information.

Course Level
Basic. Program knowledge level most beneficial to CPAs new to a skill or an attribute. These individuals are often at the staff or entry level in organizations, although such programs may also benefit a seasoned professional with limited exposure to the area.

Prerequisites
None.

Advance Preparation
None.

Course Expiration
AICPA and NASBA Standards require all Self-Study courses to be completed and the final exam submitted within 1 year from the date of purchase as shown on your invoice. No extensions are allowed under AICPA/NASBA rules.

Key Terms

- **Computer Crime:** An illegal act conducted using a computer or electronic device.
- **Computer Virus:** A computer virus is usually hidden in a computer program and performs functions such as copying or deleting data files. A computer virus creates copies of itself that it inserts in data files or other programs.
- **Computer Worms:** A computer worm is a type of malware that transmits itself over networks and the internet to infect more computers with the malware.
- **Data Breach:** The release or taking of data from a secure source to an unsecured third-party location (Computer).
- **Firewalls:** Are hardware or software designed to prevent malware from being installed on a computer and to prevent unauthorized access to a computer system.
- **Fraud:** A deception deliberately practiced in order to secure unfair or unlawful gain.
- **Hacker:** Someone attempting to gain access to a computer for malicious or illegal purposes.
- **Identifying Information:** Information such as a name, phone number, address or Social Security Number that can be used to identify an individual.
- **Internal Controls:** A process, effected by an entity's board of directors, management, and other personnel, designed to provide reasonable assurance regarding the achievement of objectives relating to operations, reporting, and compliance.
- **Malware:** Malware is placed on computers or cell phones to hijack the computers, steal data, or encrypt the data for ransom.