



Wolters Kluwer

Identity Theft & Data Security for Accountants Course Instructions

Author: Stephen Yoss

Copyright © 2019 CCH CPELink



NASBA - Sponsor number: 103021

Wolters Kluwer, CCH is registered with the National Association of State Boards of Accountancy (NASBA) as a sponsor of continuing professional education on the National Registry of CPE Sponsors. State Boards of Accountancy have the final authority on the acceptance of individual course for CPE credit. Complaints regarding registered sponsors may be submitted to the National Registry of CPE Sponsors through its website: www.nasbregistry.org.

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: January 2019

Course Description

Identity theft is the fastest growing crime in America with approximately 10 million occurrences every year. On average, it will cost the victim several hundred dollars and dozens of hours to resolve. It can cause irrevocable damage to an organization's public opinion and reputation. This course will examine the major causes, factors, and outcomes of identity theft and organizational security breaches.

Participants will be presented with current examples from a wide range of industries and attack types. This course will describe how to identify when theft occurs, what information is most at risk, where the stolen information is used, and best practices on how to prevent it from occurring. Critical Tips for Avoiding Identity Theft and Information Security Breaches is recommended for anyone concerned about their online safety and responsible for safeguarding their organizational data.

Learning Objectives

Upon successful completion of this course, participants should be able to:

- Identify and classify potential threats in technology areas, which leave organizations susceptible to privacy breaches, data theft, and distribution
- Describe how some of the larger incidents of mass identity theft occurred, the victim groups and impact
- Recognize how to build an action plan to safeguard personal and organizational data from potential threats
- Identify and implement data security best practices for their personal and organizational information
- Identify and locate resources for assisting in resolve identity theft
- Describe identity theft statistics
- Recognize types of TOR service
- Identify a marketing term that can only be initiated by credit monitoring agencies
- Identify a physical device or software package that prevents unauthorized access into or out of a network
- Identify types of internet-based data backup solution
- Recognize the estimated hours it takes the average victim to resolve each identity theft crime
- Identify something you should do immediately after realizing you're the victim of identity theft
- Describe the primary government agency for managing identity theft crimes
- Identify a security recommendation with respect to identity theft

NASBA Field of Study

Computer Software & Applications. Some state boards may count credits under different categories—check with your state board for more information.

Course Level

Overview. Program knowledge level that provides a general review of a subject area from a broad perspective. These programs may be appropriate for professionals at all organizational levels.

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

- **Enforced Antivirus:** A software to detect and remove malware from a computer.
- **Equifax:** One of three U.S. consumer credit reporting agencies.
- **Firewall:** A physical device or software package that prevents unauthorized access into or out of a network.
- **Identify Theft:** The fraudulent practice of using another person's name and personal information to obtain credit, loans, etc.
- **Medical Identity Theft:** Occurs when a perpetrator uses a victim's name, health insurance information, or identifying information to see a doctor, get prescription drugs, file a health insurance claims, or get other care.
- **Virtual Private Network:** Extends a private network across a public network and enables users to send and receive data across shared or public networks as if their computing devices were directly connected to the private network.