BEACON HILL
FINANCIAL EDUCATORS®

51A Middle Street, Newburyport, MA 01950
Phone: 800-588-7039
contact@bhfe.com www.bhfe.com

## Course Information

**Course Title:** *Information Security: Networks* *#700924*

### Recommended CPE credit hours for this course

In accordance with the standards of the National Registry of CPE Sponsors, and the Internal Revenue Service, CPE credits have been granted based on a 50-minute hour.

**CPA** **8** (Accepted in all states) .
National Registry of CPE Sponsors ID Number: 107615.
Sponsor numbers for states requiring sponsor registration:
Florida Division of Certified Public Accountancy: 0004761 (Ethics #0011467)
Hawaii Board of Public Accountancy: 14003
New York State Board of Accountancy (for ethics): 002146
Ohio State Board of Accountancy: CPE .51 PSR
Pennsylvania Board of Accountancy: PX178025
Texas State Board of Accountancy: 009349

**EA, OTRP** **8** IRS: Qualified Sponsor number: FWKKO.

### Course Description

Internal control requires that the information systems in a company are secure, reliable, and can be trusted. Cyberattacks and data breaches represent one of the greatest threats to a companies information systems. This course covers the importance of network security for all types of businesses and practices. The course will:

- Identify the vulnerabilities and define safeguards for computers, networks, networking components, software applications, and mobile devices.
- Describe the threats that can compromise computers and company data such as viruses, trojans and phishing.
- Describe some simple steps that users can take to properly protect themselves from any threats that penetrate the network and protect confidential company data.
- Discuss how to create a data security plan and an information security risk management plan along with some recommendations and best-practices for keeping networks safe.

- **Course Content**
- Publication/Revision date: 9/23/2024.
- Course author:Andrew Clark, EA
- Final exam (online): Forty questions (multiple-choice).

**Program Delivery Method:** Self-Study (NASBA QAS Self-Study/Interactive)

### Subject Codes/Field of Study

NASBA (CPA): Information Technology; IRS (EA, OTRP): Federal Tax Law.

### Course Level, Prerequisites, and Advance Preparation Requirements

Program Level: NASBA/CPA, IRS: Intermediate.
Prerequisites: None
Advance Preparation: None

## Learning Objectives

At the end of this video course, students will be able to:

- Identify the importance of network security for CPAs and Tax Practitioners.
- Identify what a network is along with the different components that make up a network.
- Identify the different types of network security that contribute to a comprehensive information security protocol.
- Define the term "identify theft" and recognize how identify theft most commonly occurs.
- Recognize why CPAs and Tax Professionals are being targeted by cybercriminals.
- Recognize the importance of encrypting client data.
- Identify the importance of creating internal controls and a security plan to protect client data.

### Instructions for Taking This Course

- **Log in to your secure account at www.bhfe.com. Go to "My Account."**
- **You must complete this course within one year** of purchase (If the course is "Expired," contact us and we will add the latest edition of the course to your account (no charge).
- **To retain the course-PDF after completion (for future reference) and to enable enhanced navigation:** From "My Account," Download and save the course-PDF to your computer. This will enable the search function (Menu: Edit>Find) and bookmarks (icon on left side of document window).
- **Complete the course by** following the learning objectives listed for the course, studying the text, and, if included, studying the review questions at the end of each major section (or at the end of the course).
- **Once you have completed studying the course** and you are confident that the learning objectives have been met, answer the final exam questions (online).

### Instructions for Taking the Online Exam

- **Log in to your secure account at www.bhfe.com. Go to "My Account."**
- A passing grade of at least **70% is required on the exam** for this course.
- You will have three attempts to pass the exam (call or email us after three unsuccessful attempts for instructions).
- The exam is not timed, and it does not need to be completed in one session.
- For a printed copy of the exam questions, open the exam and press "Print Exam."
- Once you pass the exam, the results (correct/incorrect answers) and certificate of completion appear in "My Account." A confirmation email is also sent.
- CFP Board and IRS credit hours, if applicable, are reported on Tuesdays and at the end of the month.

**Have a question?** Call us at 800-588-7039 or email us at contact@bhfe.com.

Copyright 2024 by Tax CE Publishing. All rights reserved. No part of this work may be used, reproduced, or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording, or by any information storage and retrieval system, without prior agreement and written permission from Tax CE Publishing and Andrew Clark Enterprises. The contents of this program are subject to revision without notice due to the continued evolution of the U.S. Tax Code. This program is presented as is, without warranty of any kind, including but not limited to implied warranties of the workbook's quality, performance, merchantability, or fitness for any particular purpose. Tax CE Publishing shall not be liable to the purchaser or any other entity with respect to liability, loss, or damage caused directly or indirectly by using this program. All brand names, trademarks, and registered trademarks are the property of their respective holders. Tax CE Publishing, 1890 Junction Blvd. Apt. 2515, Roseville, CA  95747.

# Table of Contents

Course Information ........ ii

Learning Objectives ........ iii

Table of Contents ........ v

Information Security ........ 1

What is a computer network? ........ 1

Network Technologies ........ 2

- Wired Network Technologies ........ 2
- Wireless Network Technologies ........ 4
- IEEE 802.11 ........ 4
- IEEE 802.11b ........ 4
- IEEE 802.11g ........ 5
- IEEE 802.11n ........ 5
- IEEE 802.11ac ........ 5
- IEEE 802.11ax ........ 5

Network Components ........ 6

- Network hubs ........ 6
- Network Switches / Bridges ........ 6
  - Network Switching ........ 8
- Network Routers ........ 8
  - Hybrid Devices ........ 9
  - What is Routing? ........ 9
  - Routing Data Packets ........ 9
  - Identifying Reachable Networks ........ 9
  - Routing Metrics ........ 9
  - Network Protocols ........ 11
- Wireless access points ........ 11
  - Access Point Modes ........ 12
  - Multiple Access Points ........ 13
  - Wireless Routers ........ 13

Internet ........ 13
Information Security ........ 14
Application security ........ 15
Incident response ........ 17
Vulnerability management ........ 18
Why Worry about Network Security? ........ 18
Information Security Risk Management ........ 19
Risk Control ........ 21
Security Concepts ........ 22
Confidentiality ........ 23
Integrity ........ 23
Availability ........ 23
People Accessing Information ........ 24
Authentication ........ 24
Authorization ........ 24
Nonrepudiation ........ 25
Unsecured Computers and Networks ........ 26
Types of Network Security ........ 27
Access Control/Network Access Control (NAC) ........ 27
Antivirus and/or Antimalware Software ........ 28
Application Security ........ 28
Behavioral Analytics ........ 29
Data Loss Prevention ........ 30
Email Security ........ 32
Email Security - Best Practices for Companies ........ 35
Email Security - Best Practices Best Practices for Individual Users ........ 39
Firewalls ........ 41
Intrusion Prevention Systems (IPS) ........ 42
Mobile Device Security ........ 43
Network Segmentation ........ 43
Physical Security ........ 44
Virtual Private Network (VPN) ........ 45
Web Security ........ 46

Web Application Security ........ 46

Wireless Security ........ 47

Disposing of Equipment Securely ........ 48

Techniques for Removing Information ........ 49

Deleting information ........ 49

Overwriting information ........ 49

Secure Erasure ........ 50

Physical destruction ........ 50

Disposing of Mobile Phones and Tablets ........ 50

Network Threats ........ 51

Review Questions ........ 53

Review Questions Answers ........ 56

Phishing ........ 61

Spear Phishing ........ 62

Clone Phishing ........ 63

Whale Phishing ........ 63

Social Media Phishing ........ 63

Phishing Evolution ........ 64

Phishing Opportunities ........ 64

Criminals are Learning and Evolving ........ 65

Phishing Tools ........ 65

Bots/Botnets ........ 65

Phishing Kits ........ 65

URL Obfuscation ........ 66

Simple HTML redirection ........ 66

Use of JPEG images ........ 66

Use of alternate IP addresses ........ 66

Registration of similar domain names ........ 67

Web Browser Vulnerabilities used for Phishing ........ 67

Session Hijacking ........ 67

Domain Name Resolving Attacks ........ 68

Global DNS Hijacking Campaign ........ 68

Cross-Site Scripting Attacks ........ 69

Domain Name Typos ........ 69
Man-in-the-Middle Attacks ........ 70
Phishing-Related Malware Examples ........ 70
Bancos ........ 70
Bankash ........ 70
W32/Grams ........ 71
CoreFloo ........ 71
Dyre Banking Malware ........ 71
Phishing Mitigations ........ 72
Phishing Solutions ........ 72
Prevent Phishing Attacks: ........ 72
Two-factor authentication ........ 73
Identify Theft ........ 74
Identify Theft Methods ........ 74
Trash Sifting/Dumpster Diving ........ 74
Mail Theft ........ 75
Address Manipulation: ........ 76
Skimming ........ 76
Scanning ........ 77
Straightforward Theft: ........ 77
Conning ........ 78
Identify Theft Crimes ........ 78
Yahoo Data Breach ........ 78
Equifax breach ........ 79
Target Data Breach ........ 79
Malware ........ 80
Viruses and Worms ........ 81
Virus ........ 81
Worm ........ 81
Trojans ........ 82
Backdoor / Remote Access Trojan (RAT) ........ 82
Botnets ........ 83
Adware ........ 86

Information stealers........86
Ransomware........86
Rootkits........87
Downloaders or Droppers........87
File Wipers........88
Spyware........88
Malware Summary........89
Data security plan........89
Complying with the Safeguards Rule........90
Who Must Comply?........90
How To Comply........91
Securing Information........91
Employee Management and Training.........92
Information Systems.........92
Detecting and Managing System Failures.........94
Creating an Information Security Risk Management Plan........95
Identify Risks........96
Perform Risk Analysis........98
Plan Risk Responses........101
Implement Risk Responses........102
Monitor Risks........102
Basic Security Training........103
Use Security Software........104
Avoid Phishing and Malware........104
Protect Personal Information........105
Mobile Phone Security........105
Mobile Phone Theft........106
Securing Mobile Phones........106
Installing Apps with Malware........107
E-mail attachments........107
SMS links........107
Keeping Your Network and Information Safe........108
Install operating system updates regularly........108

Run Antivirus software on all computers and run regular scans ........ 109

Keep Antivirus software updated ........ 109

Practice safe online activities ........ 110

Use both network firewalls and personal firewalls on all computers ........ 110

Implement enhanced security features to better protect sensitive information ........ 110

Encrypt Client Data ........ 111

Back up all data regularly ........ 112

Create Strong Passwords ........ 112

Making Passwords More Secure ........ 113

Password Managers ........ 114

Making Online Accounts More Secure ........ 115

Review Questions ........ 116

Review Question Answers ........ 120

Glossary ........ 128