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: Basic Safeguards* *#700824*

Recommended CPE credit hours for this course

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

CFP® **4.5**

CPA **6** (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 **6** IRS: Qualified Sponsor number: FWKKO.

Course Description

All CPAs and Tax Practitioners deal with very sensitive client data. Cybercriminals are highly sophisticated, well-funded, and technologically adept at hacking computers and sealing information. CPAs and tax practitioners are some of their most highly desired targets. Cybercriminals desire the client data of all CPAs and tax practitioners. If these cybercriminals can successfully obtain the client information of CPAs and tax practitioners, they can file fraudulent tax returns for refunds or commit identify theft. As a result, all CPAs and tax practitioners must protect their client's information by protecting their computers, networks and by taking some simple safety approaches. This course will define information security, describe the numerous types of threats that exist today and define how to protect your computer systems and networks to keep client data safe.

Course Content

Publication/Revision date: 3/29/2024.
Course author:Andrew Clark, EA
Final exam (online): Thirty questions (multiple-choice).

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

Subject Codes/Field of Study

NASBA (CPA), CFP Board: Taxes.
IRS (EA, OTRP): Federal Tax Law.

Course Level, Prerequisites, and Advance Preparation Requirements

Program Level: NASBA/CPA, CFP Board, IRS: Intermediate.
Prerequisites: Basic familiarity with federal taxation
Advance Preparation: None

Learning Objectives

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

- Identify the importance of information security for CPAs and Tax Practitioners,
- 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, and
- Recognize the actions that must be taken in the event of a breach of sensitive client identity 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 2023 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 1

Learning Objectives 2

Table of Contents 3

Information Security 8

Internet 8

Information Security Tools and Processes 9

Application security 9

Cloud security 10

Cryptography 10

Infrastructure security 11

Incident response 11

Vulnerability management 12

Security Concepts 12

Confidentiality 12

Integrity 13

Availability 13

People Accessing Information 13

Authentication 14

Authorization 14

Nonrepudiation 14

Information Security Risk Management 15

Risk Control 17

Unsecured Computers and Networks 18

Identify Theft 19

Identify Theft Methods 20

Trash Sifting/Dumpster Diving 20

Mail Theft 21

Address Manipulation: 21

Skimming 22

Scanning 23

Straightforward Theft: 23

Conning 23

Identify Theft Crimes 24

Yahoo Data Breach 24

Equifax breach 24

Target Data Breach 25

CPAs and Tax Practitioners are Being Targeted 25

Six Basic Safeguards 26

Install Operating System Updates 26

Antivirus Software 27

Malware Definition 29

Viruses and Worms 30

Virus 30

Worm 31

Trojans 31

Backdoor / Remote Access Trojan (RAT) 32

Botnets 32

Adware 35

Information stealers 35

Ransomware 35

Rootkits 36

Downloaders or droppers 36

File Wipers 37

Spyware 37

Malware Summary 38

Review Questions 39

Review Question Answers 42

Phishing 47

Spear Phishing 48

Clone Phishing 49

Whale Phishing 49

Social Media Phishing 50

Phishing Evolution 50

Phishing Opportunities 50

Criminals are Learning and Evolving 51
Phishing Tools 51
Bots/Botnets 51
Phishing Kits 51
URL Obfuscation 52
Simple HTML redirection 52
Use of JPEG images 52
Use of alternate IP addresses 52
Registration of similar domain names 53
Web Browser Vulnerabilities used for Phishing 53
Session Hijacking 53
Domain Name Resolving Attacks 54
Global DNS Hijacking Campaign 54
Cross-Site Scripting Attacks 55
Domain Name Typos 55
Man-in-the-Middle Attacks 56
Phishing-Related Malware Examples 56
Bancos 56
Bankash 56
W32/Grams 57
CoreFloo 57
Dyre Banking Malware 57
Phishing Mitigations 57
Phishing Solutions 58
Prevent Phishing Attacks: 58
Firewalls 59
Two-factor authentication 60
Backup software/services 60
Drive encryption 60
Data security plan 61
Complying with the Safeguards Rule 62
Who Must Comply? 62
How to Comply 62

Securing Information 63

Employee Management and Training. 63

Information Systems. 64

Detecting and Managing System Failures. 65

Creating an Information Security Risk Management Plan 66

Identify Risks 67

Perform Risk Analysis 69

Plan Risk Responses 71

Implement Risk Responses 73

Monitor Risks 73

Basic Security Training 74

Use Security Software 75

Avoid Phishing and Malware 75

Protect Personal Information 76

Mobile Phone Security 76

Mobile Phone Theft 77

Securing Mobile Phones 77

Installing Apps with Malware 77

E-mail attachments 78

SMS links 78

Create Strong Passwords 78

Making Passwords More Secure 79

Password Managers 80

Making Online Accounts More Secure 80

Securing Data Networks. 81

Install Operating System Updates Regularly. 81

Run Antivirus Software on all Computers and Run Regular Scans 82

Keep Antivirus Software Updated 82

Practice Safe Online Activities 83

Use Both network Firewalls and Personal Firewalls 83

Implement Secure Passwords and Enhanced Security Features 84

Encrypt Client Data 84

Back Up all Data Regularly 85

Email Security ... 85

Email Security- Best Practices for Companies ... 85

Email Security - Best Practices for Individual Users ... 89

Intrusion Prevention Systems (IPS) ... 92

Mobile Device Security ... 93

Network Segmentation ... 93

Virtual Private Network (VPN) ... 94

Physical Security ... 95

Disposing of Equipment Securely ... 95

Techniques for Removing Information ... 96

Deleting information ... 96

Overwriting information ... 97

Secure Erasure ... 97

Physical destruction ... 98

Disposing of Mobile Phones and Tablets ... 98

Signs of Data Theft ... 99

Data Theft Clues ... 100

What Happens if you are Hacked? ... 100

Preliminary steps include: ... 100

Data Loss Reporting ... 102

Review Questions ... 103

Review Question Answers ... 105

Glossary ... 110

Index ... 114