



BEACON HILL
FINANCIAL EDUCATORS

51A Middle Street Newburyport MA 01950

Phone: 800-588-7039 Fax: 877-902-4284

contact@bhfe.com

www.bhfe.com

Course Information

Course Title: *Keeping-Taxpayer-Data-Secure #292222*

Number of continuing education credit hours recommended for this course:

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

EA, OTRP 2 (All States) IRS: Qualified Sponsor number: *FWKKO*.

CFP® 2 CFP Board Sponsor ID #1008 (CFP Board Course ID# 257134)

CPA: 2.5 (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: 4761 (Ethics #11467)

Hawaii Board of Public Accountancy: 14003

New York State Board of Accountancy (for ethics): 002146

Ohio State Board of Accountancy: M0021

Pennsylvania Board of Accountancy-#PX178025

Texas State Board of Accountancy: 009349

Course Description

The annual global cost of cybercrime is high and getting higher all the time. In fact, cyber criminals reap a windfall from their activities that is estimated to have been \$450 billion in 2015 and is anticipated to climb to an annual \$10.5trillion average by 2025. In the United States alone, the FBI received reports of 791,790 complaints involving \$4.2 billion in 2020. Almost all of that cybercrime began with—and continues to start with—a social engineering concept known as “phishing.”

Certain business organizations, among which are those referred to as “financial institutions,” are charged by the FTC with taking particular steps to protect their customers’ financial information. Included in the category of financial institutions are professional tax preparers. Professional tax preparers normally maintain a significant amount of taxpayer information in various files—electronic and paper—that would be a treasure trove for cyber criminals.

In this course, tax preparers are introduced to the problem of cybercrime and its costs, offered methods that can be expected to reduce the chances of becoming a cybercrime victim, and informed of proper steps to take if they do become victims of cybercrime. Accordingly, it will examine cybercrime and will discuss:

- The extent of the cybercrime problem;
- The potential costs to a tax preparer whose taxpayer data have been breached;
- The best practices a tax preparer may implement to avoid becoming a cybercrime victim; and
- What a tax preparer should do if its taxpayer data has been breached.

Course Content

- Publication/Revision date: 1/14/2022.
- Author: Paul J. Winn CLU ChFC
- Final exam (online): Fifteen questions (multiple-choice).

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

Subject Codes/Field of Study

CFP Board, NASBA (CPA): Taxes.

IRS (EA, OTRP): Federal Tax Law.

Course Level, Prerequisites, and Advance Preparation Requirements Program Level

CFP Board, NASBA/CPA, IRS: Overview.

This program is appropriate for professionals at all organizational levels.

Prerequisites: None

Advance Preparation: None

Learning Objectives

Upon completion of this course, you should be able to:

- Recognize the pervasiveness of cybercrime;
- Identify the potential costs of experiencing a data breach;
- Understand the best practices that may be implemented to protect a tax preparer from cybercrime; and
- List the responsibilities of a tax preparer who has experienced a taxpayer data breach.

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 2022 by Paul J. Winn CLU ChFC. *ALL RIGHTS RESERVED.* NO PART OF THIS COURSE MAY BE REPRODUCED IN ANY FORM OR BY ANY MEANS WITHOUT THE WRITTEN PERMISSION OF THE PUBLISHER.

All materials relating to this course are copyrighted by Paul J. Winn CLU ChFC. Purchase of a course includes a license for one person to use the course materials. Absent specific written permission from the copyright holder, it is not permissible to distribute files containing course materials or printed versions of course materials to individuals who have not purchased the course. It is also not permissible to make the course materials available to others over a computer network, Intranet, Internet, or any other storage, transmittal, or retrieval system. This document is designed to provide general information and is not a substitute for professional advice in specific situations. It is not intended to be, and should not be construed as, legal or accounting advice which should be provided only by professional advisers.

Contents

Course Information	ii
Learning Objectives	iii
Contents	v
Introduction to the Course	1
Learning Objectives.....	1
Chapter 1 – Introduction to Cybercrime	2
Introduction	2
Chapter Learning Objectives.....	2
The Nature of Cybercrime	2
Computer Viruses.....	2
Denial-of-Service Attacks	3
Installing Malware	3
Trojan Horses	3
Ransomware.....	4
Spyware.....	4
Phishing.....	4
Staying Current on Cyberthreats & Avoidance Strategies	7
FBI Internet Crime Report.....	7
Summary.....	8
Chapter Review	9
Chapter 2 – Laws & Regulations Safeguarding Taxpayer Data	10
Introduction	10
Chapter Learning Objectives.....	10
The Gramm-Leach-Bliley Financial Modernization Act.....	10
FTC Standards for Safeguarding Customer Information Rule.....	10
Meeting FTC Safeguards Rule Requirements	11
FTC Privacy of Consumer Financial Information Rule	11
Requirements under the Privacy Rule	11
Individuals Who Must Receive a Privacy Notice	11
Consumer Defined.....	11
Customer Defined	12
Privacy Notices must be sent to Customers	12
Consumers Who Are Not Customers	12
The Contents of the Privacy Notice	13
The Appearance of the Privacy Notice.....	13
Safeguarding NPI.....	13
Delivering Privacy Notices	14
Opt-Out Notices.....	14
Exercising the Opt-Out Right	14
The Shelf Life of an Opt-Out Direction	14
Exceptions to the Notice and Opt-Out Requirements.....	14
Exception to the Opt-Out Requirement: Service Providers and Joint Marketing	15
Sarbanes-Oxley Act of 2002	15
Penalties for Unauthorized Disclosure or Use of Taxpayer Information	15
Code of Federal Regulations §301.7216.1	15

Internal Revenue Code §6713	16
Internal Revenue Procedure 2007-40	16
Summary	16
Chapter Review	18
Chapter 3 – The Costs of a Data Breach	19
Introduction	19
Chapter Learning Objectives	19
Data Breach	19
Causes of Data Breach	19
Cybercrime Costs	19
IBM-Ponemon Study	20
Customer Loss	21
Number of Records Stolen or Compromised	21
Time Required to Identify and Contain a Data Breach	21
Cause of the Data Breach	22
Remediation and Other Costs Following Identification of Breach	22
Probability of Experiencing a Data Breach	23
Summary	23
Chapter Review	24
Chapter 4 – The Information Security Plan.....	25
Introduction	25
Chapter Learning Objectives	25
Ensuring Data Security	25
Where to Begin: Determining Responsibility	26
Identifying the Risks and Their Impact.....	26
Writing an Information Security Plan	26
Securing the Physical Facility	27
Personnel Security.....	27
Protection of Data from Human Error	28
Protection of Data from Intentional Compromise or Loss.....	28
Information and Computer Systems Security	29
Media Security	30
Summary	30
Chapter Review	31
Chapter 5 – Best Practices for Securing Data	32
Introduction	32
Chapter Learning Objectives.....	32
Recommended Practices	32
Employee Management	32
Employee Training	33
Policies and Procedures	33
Maintaining Information System Security	33
Information Storage	33
Protecting against Unauthorized System Access	34
Detecting Possible Improper Disclosure	34
Customer Data Transmission	34
Disposal of Customer Information.....	34
DOL Best Practice Guidance.....	35
That guidance in its entirety, and other advice for maintaining data security may be accessed at https://www.dol.gov/newsroom/releases/ebsa/ebsa20210414.Summary	35
Chapter Review	36
Chapter 6 – When a Data Breach Occurs.....	37
Introduction	37

Chapter Learning Objectives	37
When a Data Breach Occurs	37
Secure the Firm’s Operations.....	37
Remove Improperly Posted Information from the Web	38
Interview	38
Fix Vulnerabilities.....	38
Thinking about Service Providers.....	39
Checking the Firm’s Network Segmentation	39
Working with Forensics Experts	39
The Firm’s Communications Plan	39
Notify Appropriate Parties	39
Notify Law Enforcement	39
Notify Affected Businesses.....	39
Notify Individuals	40
Model Letter	41
Summary	43
Chapter Review	44
Glossary	45
Answers to Review Questions.....	47
Chapter 1.....	47
Chapter 2.....	48
Chapter 3.....	48
Chapter 4.....	49
Chapter 5.....	49
Chapter 6.....	50
Index	51
Appendix I.....	2
Appendix II	3
Social Security number	3