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

Course Information

Course Title: *Information Security: Malware #701023*

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 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
Pennsylvania Board of Accountancy: PX178025
Texas State Board of Accountancy: 009349

EA, OTRP 6 IRS: Qualified Sponsor number: FWKKO.

Course Description

The malware and cybersecurity landscapes are constantly shifting in response to the actions of one another. On one side, cybersecurity experts are identifying, analyzing, and patching new forms of malware as consistently as possible so they can be detected by antivirus software and purged from infected systems before they can cause harm to their potential victims. On the other side, malware creators and cybercriminal organizations are constantly creating new malware, and altering old malware, to circumvent cybersecurity efforts and continue to infect as many computers as possible for a variety of purposes.

This course will:

- Identify the overarching concepts that make up the current information security landscape;
- Provide an overview of the different types of malware that can infect a computer system as well as the different techniques used to conduct both phishing attacks and identity theft;
- Identify the general malware trends over the past several years and explain how the current malware landscape arrived at where it is today;

- Describe the most commonly seen pieces of malware from this year and provide both an in-depth explanation on how the malware operates and best practices to properly deal with each piece of malware.

Course Content

Publication/Revision date: 7/26/2023.
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): 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 information security for CPAs and Tax Practitioners,
- Identify the different types of malware that can infect computer systems,
- Define the term "Phishing" and recognize how phishing occurs,
- Define the term "Identify Theft" and recognize how identify theft most commonly occurs,
- Identify the major malware events that have occurred in recent years, and
- Identify the operating processes and mitigation techniques for the most commonly seen malware programs of the current year.

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 ii

Learning Objectives iii

Information Security 1

Internet 1

Information Security Tools and Processes 2

- Application security 2
- Cloud security 3
- Cryptography 4
- Infrastructure security 4
- Incident response 4
- Vulnerability management 5

Security Concepts 5

- Confidentiality 5
- Integrity 6
- Availability 6

People Accessing Information 6

- Authentication 7
- Authorization 7
- Nonrepudiation 8

Malware Definition 9

- Viruses and Worms 10
- Virus 10
- Worm 10
- Trojans 11
- Backdoor / Remote Access Trojan (RAT) 11
- Botnets 12
- Adware 15
- Information stealers 15
- Ransomware 15
- Rootkits 16
- Downloaders or droppers 16

File Wipers 17
Spyware 17
Malware Summary 18
Phishing 18
Spear Phishing 20
Clone Phishing 21
Whale Phishing 21
Social Media Phishing 21
Phishing Evolution 21
Phishing Opportunities 22
Criminals are Learning and Evolving 22
Phishing Tools 23
Bots/Botnets 23
Phishing Kits 23
URL Obfuscation 23
Simple HTML redirection 24
Use of JPEG images 24
Use of alternate IP addresses 24
Registration of similar domain names 25
Web Browser Vulnerabilities used for Phishing 25
Session Hijacking 25
Domain Name Resolving Attacks 26
Global DNS Hijacking Campaign 27
Cross-Site Scripting Attacks 27
Domain Name Typos 28
Man-in-the-Middle Attacks 28
Phishing 28
Bancos 28
Bankash 28
W32/Grams 29
CoreFloo 29
Dyre Banking Malware 29
Phishing Mitigations 30

Phishing Solutions 30
Prevent Phishing Attacks 30
Identity Theft 32
Identity Theft Methods 32
Trash Sifting/Dumpster Diving 32
Mail Theft 33
Address Manipulation: 34
Skimming 34
Scanning 35
Straightforward Theft: 36
Conning 36
Identity Theft Crimes 36
Yahoo Data Breach 36
Equifax breach 37
Target Data Breach 37
Malware Trends 38
2014 Malware Trends 38
Increases in Researcher Evasion 38
Malware Source Code Leaks 39
Changes in Account Takeover Fraud Execution 40
Mobile SMS Malware Rose in Popularity 41
Obsolete Malware Infection Techniques Started Making a Comeback 41
2015 Malware Trends 43
Mobile Banking Trojans on the Rise 43
Overlay of Malware on Top of Legitimate Applications 43
Increases in Mobile Ransomware 45
First Ransomware for Linux Detected 45
Encryption-Based Ransomware is on the Rise 46
2016 Malware Trends 47
Ransomware Solidified Itself as a Serious Threat 47
Underground Cybercriminal Marketplaces are Becoming More Common 49
$100 Million was Stolen from Banks in SWIFT-Enabled Transfers 49
BlackEnergy Wreaked Havok on Vulnerable Critical Ukrainian Infrastructure 50

Mirai Botnet Attack Shows the Vulnerability of Internet of Things (IoT) Devices 50
Mobile Adware Infections Increase Dramatically 51
2017 Malware Trends 52
Despite the Plateauing of new Ransomware Families, WannaCry and NotPetya take the Ransomware Landscape by storm 52
Mobile “Evasive” Malware is Extremely Popular and More Dangerous Than It’s Ever Been 54
Losses from Business Email Compromise and CEO Fraud Reach $5 Billion 55
2018 Malware Trends 55
Botnets Are Now Used to Attack Both Organizations and Users of Infected Computers 56
As Rooted Mobile Malware Declines in Popularity, Traditional Malware Infection Rates Surge 57
With the Rising Value of Cryptocurrency, Mining Malware is Rising in Popularity 58
2019 Malware Trends 60
WannaCry Ransomware 60
Kovter Click Fraud Malware 62
Gh0st RAT 63
NanoCore RAT 64
CoinMiner Cryptocurrency Mining Malware 66
ZeuS Modular Banking Malware 67
Emotet Infostealer 68
Trickbot Banking Trojan 71
Qakbot Financial Malware 73
Dridex Banking Trojan 75
Common Malware Threats of 2020 77
KMS 78
Dridex Banking Trojan 78
Tech Support Scams 79
Glupteba Trojan 79
Infostealers 80
Important Mentions: Trickbot and Emotet Infostealer 80
Important Malware Trends of 2021 81
Ransomware Attacks Will Continue to Increase in Both Number and Sophistication in 2021 81
Cybercriminals and Threat Actors will Continue to Exploit the COVID-19 Pandemic 82
Non-Windows Malware Attacks are Increasing 82

Vulnerabilities that Enable Malware will Likely Increase in 2021 83
Important Malware Trends of 2022 83
Healthcare Sector Cyberattacks are on the Rise 84
Ransomware Attacks are Becoming more Sophisticated and Vicious 84
Security-as-a-Service and Zero Trust Networks is on the Rise 85
Important Malware Trends of 2023 85
Ransomware Attacks Continue to Grow, but Switch Focus to Supply Chain Companies 86
Ransomware-as-a-Service Increases in Popularity 87
Zero Trust Security Systems See Wider Implementation, but still aren't Perfect 87
Review Questions 89
Review Question Answers 91
Glossary 95
Index 99