

## **OBJECTIVES**

- 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
- Recognize the actions that must be taken in the event of a breach of sensitive client identity data

## **TOPICS COVERED**

- Information Security
- Internet
- Information Security Tools and Processes
- Application security
- Cloud security
- Cryptography
- Infrastructure security
- Incident response
- Vulnerability management
- Security Concepts
- Confidentiality
- Integrity
- Availability
- People Accessing Information
- Authentication
- Authorization
- Nonrepudiation
- Information Security Risk Management
- Risk Control
- Unsecured Computers and Networks
- Identify Theft
- Identify Theft Methods
- Trash Sifting/Dumpster Diving
- Mail Theft
- Address Manipulation:
- Skimming
- Scanning
- Straightforward Theft:
- Conning
- Identify Theft Crimes
- Yahoo Data Breach
- Equifax breach
- Target Data Breach
- CPAs and Tax Practitioners are Being Targeted
- Six Basic Safeguards
- Install Operating System Updates
- Antivirus Software
- Malware Definition
- Viruses and Worms
- Virus
- Worm
- Trojans
- Backdoor / Remote Access Trojan (RAT)
- Botnets
- Adware
- Information stealers
- Ransomware
- Rootkits
- Downloaders or droppers
- File Wipers
- Spyware
- Malware Summary
- Phishing
- Spear Phishing
- Clone Phishing
- Whale Phishing
- Social Media Phishing
- Phishing Evolution
- Phishing Opportunities
- Criminals are Learning and Evolving
- Phishing Tools
- Bots/Botnets
- Phishing Kits
- URL Obfuscation
- Simple HTML redirection

- Use of JPEG images
- Use of alternate IP addresses
- Registration of similar domain names
- Web Browser Vulnerabilities used for Phishing
- Session Hijacking
- Domain Name Resolving Attacks
- Global DNS Hijacking Campaign
- Cross-Site Scripting Attacks
- Domain Name Typos
- Man-in-the-Middle Attacks
- Phishing-Related Malware Examples
- Bancos
- Bankash
- W32/Grams
- CoreFloo
- Dyre Banking Malware
- Phishing Mitigations
- Phishing Solutions
- Prevent Phishing Attacks:
- Firewalls
- Two-factor authentication
- Backup software/services
- Drive encryption
- Data security plan
- Complying with the Safeguards Rule
- Who Must Comply?
- How to Comply
- Securing Information
- Employee Management and Training.
- Information Systems.
- Detecting and Managing System Failures.
- Creating an Information Security Risk Management Plan
- Identify Risks
- Perform Risk Analysis
- Plan Risk Responses
- Implement Risk Responses
- Monitor Risks
- Basic Security Training
- Use Security Software
- Avoid Phishing and Malware
- Protect Personal Information
- Mobile Phone Security
- Mobile Phone Theft
- Securing Mobile Phones
- Installing Apps with Malware
- E-mail attachments
- SMS links
- Create Strong Passwords
- Making Passwords More Secure
- Password Managers
- Making Online Accounts More Secure
- Securing Data Networks
- Install Operating System Updates Regularly
- Run Antivirus Software on all Computers and Run Regular Scans
- Keep Antivirus Software Updated
- Practice Safe Online Activities
- Use Both network Firewalls and Personal Firewalls
- Implement Secure Passwords and Enhanced Security Features
- Encrypt Client Data
- Back Up all Data Regularly
- Email Security
- Email Security- Best Practices for Companies
- Email Security - Best Practices for Individual Users
- Intrusion Prevention Systems (IPS)
- Mobile Device Security
- Network Segmentation
- Virtual Private Network (VPN)
- Physical Security
- Disposing of Equipment Securely
- Techniques for Removing Information
- Deleting information
- Overwriting information
- Secure Erasure
- Physical destruction
- Disposing of Mobile Phones and Tablets
- Signs of Data Theft
- Data Theft Clues
- What Happens if you are Hacked?
- Preliminary steps include:
- Data Loss Reporting