

# Cybersecurity Defense for CPAs

| Credits<br>2.0 | Field of Study<br>Information Technology | Course Category<br>Security | Level<br>Basic |
|----------------|------------------------------------------|-----------------------------|----------------|
|----------------|------------------------------------------|-----------------------------|----------------|

## COURSE DESCRIPTION

AI has changed cybercrime faster than most firms have changed their defenses. Phishing emails now arrive error-free and personalized, often referencing real colleagues, clients, and projects. Cloned voices and deepfake video are being used to request wire transfers and banking changes. Ransomware operators use AI agents to break into networks in hours instead of weeks, and breaches increasingly come through trusted vendors and connected apps rather than a firm's own systems. This session looks at how today's attacks actually work, the scams circulating right now, and why the warning signs professionals were trained to look for no longer apply. This is not another "don't click the link" lecture. You'll see real attack patterns taken apart step by step, learn to recognize AI-generated fraud when it lands in your inbox or on your phone, and put verification habits in place that hold up even when the request looks and sounds legitimate. You'll leave with a clear picture of the threats that matter this year and a prioritized set of defenses for your firm, your staff, and your clients.

## LEARNING OBJECTIVES

- Identify AI-generated phishing emails, cloned voices, and deepfake video
- Recognize the warning signs of today's most common scams targeting accounting and finance professionals
- Apply a callback verification procedure to a payment request or banking change
- Determine where a documented ransomware or data breach attack could have been stopped
- Select the controls that most effectively reduce the risk of AI-enabled fraud, ransomware, and data breaches

## MAJOR TOPICS

- The AI-powered attacker: phishing, deepfakes, and voice cloning
- Today's scams: what's hitting accounting and finance professionals now
- Ransomware and breaches: faster attacks and the vendor back door
- Building defenses that work: verification, access controls, and staff readiness

## WHAT YOU'LL WALK AWAY WITH

- You'll spot AI-written phishing, cloned voices, and deepfake video before they fool you or your staff.
- You'll recognize the scams hitting accounting and finance professionals right now.
- You'll stop fraudulent payment requests and banking changes with a callback procedure that works even when the request looks legitimate.
- You'll see exactly where a real attack could have been stopped, and apply that to your own firm.
- You'll know which controls to put in place first to protect your firm, your staff, and your clients.

## QUESTIONS

---

### Do I need an IT or security background to take this course?

No. It's a basic-level course written for accounting and finance professionals. The focus is on recognizing attacks and putting practical defenses in place, not on technical configuration.

### Is this just another 'don't click the link' training?

No. The course looks at how today's attacks actually work, including AI-written phishing, cloned voices, deepfake video, and AI-assisted ransomware, and why the old warning signs no longer apply.

### Will I see real examples?

Yes. You'll work through examples of AI-generated fraud, current scams aimed at accounting and finance professionals, and a documented ransomware or breach attack broken down step by step.

### Does the course cover written security plans or IRS data-security requirements?

Not in depth. This session focuses on current threats and the defenses that stop them. Written information security plans and IRS requirements are covered in separate courses.

### What will I be able to put in place right away?

A callback verification procedure for payment requests and banking changes, plus a short list of the controls that most effectively reduce the risk of AI-enabled fraud, ransomware, and data breaches.

## A NOTE FROM THE AUTHOR

---

I built this course because the scams hitting accounting firms today don't look like the ones we trained people to catch. The emails are clean, the voices sound right, and the attacks move faster than most firms can react. I wrote it for professionals who need to recognize these attacks and stop them without becoming security specialists.

## ADDITIONAL INFORMATION

---

- **Who Should Attend:** CPAs and financial professionals seeking a practical foundation in modern cybersecurity.
- **Prerequisites:** None
- **Advanced Preparation:** None
- **Tags:** CPA cybersecurity update 2026, Business Email Compromise prevention, ransomware defense for accountants, social engineering awareness, AI confidentiality risks, Zero Trust for CPAs, identity management, cloud accounting security, professional liability du
- **Course ID:** 134
- **Short Name:** Cybersecurity Defense

