

# WIRE TRANSFER RED FLAGS

*One 'Quick Favor' could cost your firm \$50,000.*

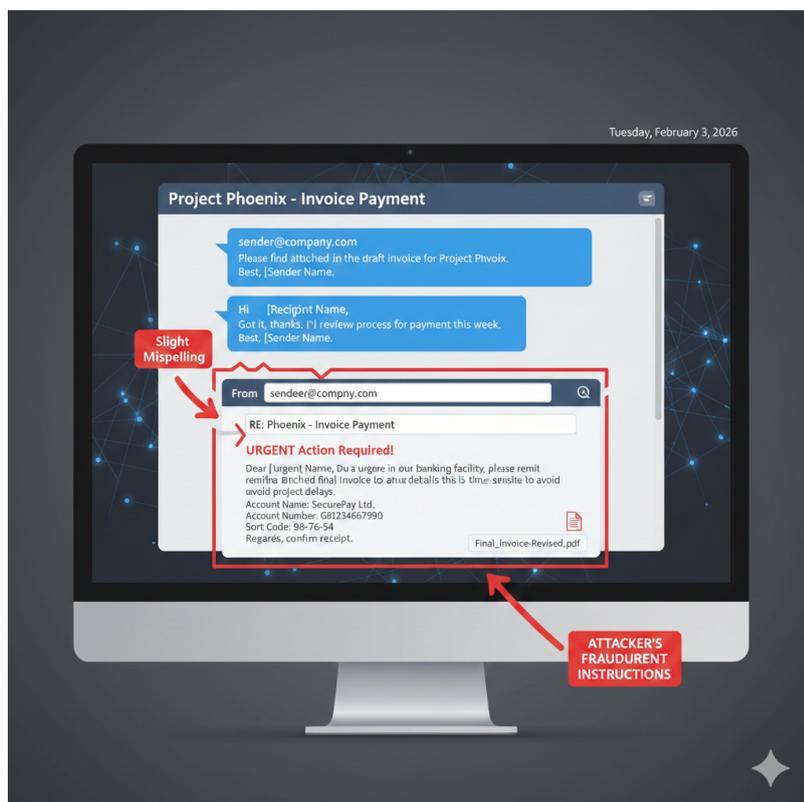
## Page 1: The Hijack Anatomy

**The Problem:** Business Email Compromise (BEC) is the #1 financially damaging threat to accounting practices. Attackers sit inside compromised accounts for months, learning your tone.

Feature	Legit Request	Hijacked Request
Tone	Professional/Typical	Unusual Urgency ("Process NOW")
Email Address	client@company.com	client@cornpany.com (look closely)
Payment Info	Matches records	New bank or "Personal" account

### [GRAPHIC: ANNOTATED EMAIL]

*Visualizing a "Thread Hijack" where the attacker replies to an existing conversation with fraudulent instructions.*



## Page 2: The Golden Rule

### The "Voice-to-Ear" Policy

No payment change is valid until you hear a known voice on the phone confirm it.

- ❑ No exceptions for "urgent" meetings or travel.
- ❑ Never use the phone number provided in the suspicious email.
- ❑ Use the "Official Number" stored in your CRM.

### CardinalsByte Action Step

**Implement DMARC/DKIM protocols today.** These technical safeguards prevent hackers from spoofing your firm's domain to your clients, ensuring your outgoing mail is verified.

## CardinalsByte

Cybersecurity Compliance & Risk for:  
Small Business, CPAs, Tax Professionals, Bookkeepers and Accountants

[www.cardinalsbytes.com](http://www.cardinalsbytes.com)