FRAUD PREVENTION · MAY 4, 2026

# How Progress-Draw Fraud Works — and the 3 Controls That Stop It

If you run a construction or engineering firm in Canada, there's a good chance you've never heard the term "progress-draw fraud" — but you've almost certainly heard the story. A supplier or subcontractor emails your accounts payable team with "updated banking details." The invoice looks right. Someone processes it. By the time anyone notices, the money is gone.

## Why construction is the perfect target

A typical Canadian project connects 15 to 40 subcontractors, each submitting invoices and draw requests through email — the least secure, least monitored channel in most small firms' operations. This isn't hypothetical: Canadian contractor Bird Construction was hit with a $9 million CAD ransomware demand in 2019.

## How the scam actually works

**Compromised subcontractor mailbox:** a fraudster gains access to a real email account and sends "updated" banking details from inside a genuine conversation.

**Look-alike domain impersonation:** a domain one character off from a real subcontractor's, timed to a real payment.

## The three controls that actually stop it

- A written payment-verification procedure — verify any banking change by phone, using a number already on file.
- MFA on every account in the payment chain — not just email.
- A second sign-off on any payment above a set threshold.