CICADA | RESOURCES

LESSON 03 OF 04 · 7 MIN · ESSENTIAL

Invoice fraud and the callback rule

The most expensive email in small business, and the twenty-minute process that stops it.

The email isn't the vulnerability

Invoice fraud often arrives from a real supplier's mailbox after it has been compromised. The thread is genuine, the invoice format is right, and only the bank details have changed. Email filters may have nothing to catch.

The vulnerability is the process: a payment instruction accepted without independent verification.

One rule, no exceptions

Any change to bank details, supplier account or payment destination is verified by a voice call to a known contact on a known number. Not a reply, not a forwarded email, not a number in the signature.

Support it with a second approver for larger payments, a verified supplier phone list kept outside email, and a culture where anyone can pause a payment without apologising.

If money has moved

Call the bank's fraud line immediately and ask for a recall. Call the real supplier on a known number. Preserve the email and headers. Report to the fraud service and notify your insurer. Don't contact the attacker's account or try to negotiate.

Speed matters more than pride. A report in ten minutes is worth far more than a perfect explanation tomorrow.

> MAKE IT PUBLIC

> Tell suppliers at onboarding: “We will always call a number we already have before changing bank details.” It sets an expectation and makes the rule easier to enforce.

Key takeaways

- ✓ Compromised supplier mailboxes make invoice fraud hard to spot by content.
- ✓ Verify every bank-detail change by phone on a known number.
- ✓ Use dual approval and a verified contact list.
- ✓ Call the bank immediately if a payment has gone.

Generated free at resources.cicadacs.com · General guidance, not an audit or legal advice.