



FULL GUIDE: INVOICE & PAYMENT FRAUD

WHY THIS GUIDE EXISTS

Most cyber security material is written for enterprises with a security team already in place. This guide isn't. It's written for businesses that run on a small team, a handful of suppliers, and a finance process built for speed, which is exactly the profile invoice and payment fraud is designed to exploit.

This isn't a story about being "hacked." In almost every case, nothing is broken into. The scam works by imitating a normal business conversation closely enough that nothing feels unusual until the money is already gone, which means the fix isn't more technology, it's a small number of habits, applied consistently.

This guide covers three things:

- How the scam actually plays out, step by step
- The red flags that give it away, if you know where to look
- Five practical habits that stop almost all of it, with no new software or budget

Fifteen minutes with this guide is a reasonable use of anyone's time. If you'd like it walked through against your own business specifically, that's what the follow-up call is for.



FULL GUIDE: INVOICE & PAYMENT FRAUD

SECTION 1 — HOW IT WORKS

These five steps are the pattern behind almost every version of this fraud, regardless of industry or company size.

01 Reconnaissance

The attacker identifies a real supplier relationship, often from a public invoice, a LinkedIn connection, or a leaked email thread and studies how that supplier normally communicates.

02 The look-alike setup

A domain is registered that looks almost identical to the real supplier's (one letter swapped, or a different ending), and an email is drafted to match the real tone and format.

03 The approach

The email arrives referencing a real invoice, a real project, or an existing thread, sometimes inserted directly into a genuine email conversation the attacker has already gained access to.

04 The ask

A routine-sounding request: updated bank details, an outstanding balance, or a payment brought forward, usually with mild urgency and no obvious red flags on a quick read.

05 The payment

Once the payment is sent to the new (fraudulent) account, it's typically moved out within hours, which is why verification has to happen before payment, not after.



FULL GUIDE: INVOICE & PAYMENT FRAUD

SECTION 2 — SPOT THE RED FLAGS

Keep this near the inbox. Most fraudulent emails give away at least one of these, if someone knows to look.

In the sender's address

- Domain is almost right, but not quite (an extra letter, a hyphen, a different ending like .co instead of .com)
- Display name looks familiar, but the address underneath doesn't match past emails from that contact
- Reply-to address is different from the visible sender address

In the message itself

- Urgency or pressure, "needs to go out today," "I'm unavailable to confirm by phone"
- A request to change bank details, payment method, or contact information
- Slightly off tone, formatting, or signature compared to previous emails from the same contact
- Asks to keep the request confidential or to bypass the usual approval process

In the request

- Any change to previously-used bank details, even for a well-known, long-standing supplier
- A payment brought forward or made outside the normal schedule
- An invoice for a product, service, or project you can't immediately place

Don't Reply

Don't reply to the email or call any number it provides, go around it entirely.

Call Direct

Call the supplier or colleague directly, using a number you already have on file.

Flag It

Flag it to whoever handles this in your business, even if you're not fully sure.

SECTION 3 — PROTECT YOUR BUSINESS

None of these require new software, a security team, or a budget line, just a consistent habit across the team.

01 Verify by phone, not by email

Any request to change bank details or payment instructions gets confirmed by a phone call to a known, previously-used number, never a number or reply-to address supplied in the email itself.

02 Add a second approver for payments over a set amount

Pick a threshold that makes sense for your business and require a second person to sign off before it goes out. This single habit stops the majority of successful invoice fraud attempts.

03 Slow down on urgency

Treat urgency itself as a reason to double-check, not a reason to skip the check. Real suppliers can wait for a phone call.

04 Check the actual sender address, not just the display name

The display name can say anything, the address underneath is what matters.

05 Know who to call if something looks wrong

Have one person or number that any staff member can flag a suspicious email to, without worrying about looking overly cautious.

If you'd like a straight read on where your own business would be exposed against these five habits, a short, no-obligation call is the easiest way to find out, no pitch, just a clear picture.



Schedule a Call