



SEE HOW IT WORKS

WHY IT MATTERS

These scams rarely involve any system being "hacked." They work by imitating a normal business conversation closely enough that nothing feels unusual until the money is already gone. Recognizing the pattern is most of the battle.

HOW THE SCAM PLAYS OUT

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 the verification step has to happen before payment, not after.

NEVER CAUGHT OFF-GUARD

None of these steps require sophisticated hacking, just patience and a convincing enough imitation. That's exactly why a simple verification habit is so effective against it.

If you'd like a walkthrough of what this looks like for your specific business, a short call is the fastest way to get one, no pitch, just a clear picture.



Schedule a Call

Trust Akita with your cybersecurity needs. akitacyber.com | Precision. On point. On target. Every time.