



SPOT THE RED FLAGS

WHY IT MATTERS

Most fraudulent emails give away at least one warning sign, if someone knows to look. Keep this checklist near the inbox, it takes seconds to check and it stops the majority of attempts.

WHAT TO WATCH FOR

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

IF YOU SPOT ONE

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.

If you'd like this turned into a one-page poster for your team, or want to talk through your current process, a short call is a good next step.

Schedule a Call

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