Analysis report — sample

Sample data · no real information

PHISHING / BEC **Score:** 96/100 **Priority:** P1 **Max severity:** Critical

Email details

Subject	REQUEST TO UPDATE BANKING DETAILS
From	"Finance Department" <ceo.urgent@gmail.com>
To	treasury@yourcompany.com
Date	Mon, 19 May 2026 10:26

Detected findings

CRITICAL	R-BEC-008	Body mentions the company but the sender is external (gmail.com)
CRITICAL	R-CNT-006	Request to change banking / payroll details
HIGH	R-BEC-002	Display name does not match the real account
MEDIUM	R-BEC-003	Professional display name from a free email provider

Indicators of compromise (IOC)

Sender	ceo.urgent@gmail.com
Look-alike domain	yourcompany-payments[.]com (registered 4 days ago)
Fraudulent IBAN	ES?? ???? ???? ?? ???????? (changed from the usual one)

Recommended actions

1. Do not make any transfer or IBAN change without phone confirmation via a known channel.
2. Report the email as phishing and purge copies delivered to other mailboxes.
3. Block the look-alike domain in the proxy and anti-phishing policies.
4. Open a P1 ticket in the incident module and warn the impersonated person.