

Smishing: Text Messages Impersonating Spanish Institutions

A text message signed by the Spanish Tax Agency, Correos, Social Security or your bank can look identical to the real thing. There is no signature to check and no domain to inspect, just a short number and a link. That ordinariness is why smishing turns an SME into a victim within seconds.

A lure that sounds routine

The message asks for a customs fee to release a parcel, a tax refund to claim, a blocked account to reactivate, or a traffic fine to pay. None of these feel out of place for a company that receives parcels, files taxes and runs payroll every month. The link opens a page copying the official design and asks for login credentials or card details.

Why SMS deceives better than email

- There is no mechanism confirming who sent a text, unlike email with SPF and

DKIM.

- The message lands in the same thread as legitimate courier or bank notifications.
- The small screen hides the real domain and pushes a decision in seconds, with less room to doubt than email phishing or phone vishing.

What an employee should do

Do not tap the link or call the number in the message. Verify the matter by going directly to the official website or the bank's app, never from the text itself. If something feels off, forward it to the internal reporting channel instead of just deleting it.

What the company should have in place

- A reporting channel everyone knows about, with a fast response.

Want to know if your company is truly protected?

Ciphraverse helps SMEs turn technical findings, regulatory pressure and client questionnaires into clear security decisions.

Explore services on ciphraverse.com



Ciphraverse Checked

The visible sign of a serious commitment to security.