DIGITAL PRESENCE

The Official Page Your Customers Can Check Before They Pay

In 2026 several scams in Venezuela borrowed real events and real names. On 26 June the Asociación Bancaria de Venezuela (ABV), the banking association, warned of fake portals trying to exploit the emergency caused by the earthquakes of 24 June. It asked people to give only to organisations with a current legal registration and not to send mobile payments (pago móvil) to individuals' accounts.

The ABV's warning was published by Finanzas Digital on 26 June 2026.
https://finanzasdigital.com/alertan-fraudes-donaciones-terremoto-venezuela/

In May, Sudeban, the banking regulator, had already warned on Instagram about fraudulent links sent by email and social media, and about supposed benefits promoted through Telegram and WhatsApp. On 29 September the CICPC's cybercrime division warned of emails and text messages imitating Banco de Venezuela. They used the name Venezuela Renace, a real credit programme for rebuilding homes damaged by the earthquakes, or manipulated domains to offer pre-approved loans.

The CICPC alert is covered in El Diario's report of 29 September 2026.
https://eldiario.com/2026/09/29/estafas-credenciales-venezuela-renace/

AppGate's release on its Fraud Beat 2026 report, issued on 29 April, says brand impersonation fuelled a year-on-year phishing surge of up to 228% across Latin America's ten most-targeted countries, and cites Anti-Phishing Working Group (APWG) data showing that social platforms have become the main fraud funnel. Bloomberg Línea, citing the same report, wrote on 8 May that Venezuela was the country in the region where digital fraud grew most in 2025, by 228% year on year. This year's alerts mostly concern banks, but the method works just as well against a shop, a clinic or a distributor: a look-alike profile, a new number, an account to pay into.

The Venezuelan figure appears in Bloomberg Línea's article of 8 May 2026.
https://www.bloomberglinea.com/tecnologia/de-venezuela-a-el-salvador-los-paises-de-latam-donde-mas-aumento-el-fraude-digital/

Publish Rules Your Customers Can Check

As El Diario reported in April, Banco de Venezuela has repeated that its official communications do not include external links for verifying information. Any customer can apply a rule that short. A business can publish its own rules on an official channels page, on a domain it controls, and make

everything point there: each social bio, the email signature, WhatsApp auto-replies, invoices and packaging. The page should take a minute to read and fit on a phone screen.

- List your phone and WhatsApp numbers, the exact username on each social network and your contact email, and check that they match the ones you actually use.
- State the legal name and RIF that payments go to, with the current bank accounts and pago móvil details. If an account changes, update this page first.
- Say what you will never ask for: codes received by text message, passwords, payments to accounts not listed on this page, or visits to links on other domains.
- Explain how to report a fake profile or message, who receives the report and how quickly you reply.
- Show the date of the last review, and update the page whenever a number, an account or a member of staff changes.

Your Catalogue Should Not Live Only on a Profile

The second risk is losing the profile itself. On 15 August the national press workers' union (SNTP) reported that El Nacional's Instagram account was still suspended after fraudulent copyright claims, and that other outlets had had content removed or accounts suspended over claims the union described as false. In March, Meta announced that over the next few years it will use more advanced AI to enforce its rules, once those systems outperform its current methods, and rely less on third-party vendors; the company says people will keep a key role in appeals against disabled accounts.

The union's report was covered by El Diario on 15 August 2026.
https://eldiario.com/2026/08/15/sntp-denuncias-falsas-medios/

Those cases involve news outlets, not shops, and we know of no public count of suspended Venezuelan business accounts. Even so, if prices, photos and contact details exist only inside a profile, losing it leaves customers with nowhere to check anything. Keep the original photos and descriptions outside the platform, with a stable link for each product on your own domain. Hold the list of customers who agreed to receive updates in a system of your own. And write down what you will post, and on which channel, if the account goes down on a Friday night.

How Resilient Websites Handles It

We start with an inventory of channels: every number, username, email address and payment account, who administers it and where it appears. From that we write the official channels page and the list of things the business will never ask for, at a short address that is easy to read out. The

catalogue lives on the site, with price, date of the last update, availability and a button that opens the official WhatsApp; social profiles link to each product. The site installs on the phone as a web app (PWA) and stores that page and the catalogue, so they can be checked on a poor connection or none at all. The agreed payment flow shows the same accounts as the official page. We add an impersonation report form that reaches a named person.

> *An official page helps customers verify, but it does not stop anyone creating fake profiles or domains. Removing an impersonation or restoring a suspended account is each platform's decision, and no website can guarantee it. The figures cited belong to their authors.*

A Check You Can Run

Take a phone that is not signed in to your business accounts. Open each of your public profiles, follow the link in the bio and check that it reaches your own domain and shows the same numbers and payment accounts as your other channels. Then search each network for your business name and its common misspellings, and list any profile using your name, logo or photos that you do not control. Do not message those profiles or open their links. Report each one through the platform's own procedure: on Facebook, Report profile or Report Page from the Options menu (the three dots); Facebook also accepts these reports from people without an account. Note the date and the result, so you can repeat the search next month.

Supporting guidance: Facebook's instructions for reporting a profile or Page pretending to be you.
https://www.facebook.com/help/174210519303259

Continue with: Your Domain Should Not Depend on Someone Else's Email.
https://systems.kavaliero.com/en/blog/your-domain-should-not-depend-on-someone-elses-email

For help with this work, see the scope of Resilient Websites.
https://systems.kavaliero.com/en/services/resilient-websites