PRESENCIA DIGITAL

La Página Oficial que Tus Clientes Pueden Revisar Antes de Pagar

En 2026, varias estafas en Venezuela se apoyaron en hechos y nombres reales. El 26 de junio, la Asociación Bancaria de Venezuela (ABV) alertó sobre portales falsos que intentaban aprovechar la emergencia causada por los terremotos del 24 de junio. Pidió donar solo a organizaciones con registro legal vigente y no enviar pago móvil a cuentas de personas naturales.

La alerta de la ABV la publicó Finanzas Digital el 26 de junio de 2026.
https://finanzasdigital.com/alertan-fraudes-donaciones-terremoto-venezuela/

En mayo, la Sudeban ya había advertido en Instagram sobre enlaces fraudulentos enviados por correo y redes sociales, y sobre supuestos beneficios promocionados por Telegram y WhatsApp. El 29 de septiembre, la División de Delitos Informáticos del CICPC alertó sobre correos y mensajes de texto que simulan notificaciones del Banco de Venezuela. Usan el nombre de Venezuela Renace, un programa real de créditos para reconstruir viviendas afectadas por los sismos, o dominios manipulados para ofrecer créditos preaprobados.

La alerta del CICPC está recogida en la nota de El Diario del 29 de septiembre de 2026.
https://eldiario.com/2026/09/29/estafas-credenciales-venezuela-renace/

El comunicado de AppGate sobre su informe Fraud Beat 2026, del 29 de abril, sostiene que la suplantación de marcas impulsó un aumento interanual del phishing de hasta 228% en los diez países más atacados de América Latina, y cita datos del Anti-Phishing Working Group (APWG) según los cuales las redes sociales se convirtieron en el principal embudo del fraude. Bloomberg Línea, citando el mismo informe, publicó el 8 de mayo que Venezuela fue el país de la región donde más creció el fraude digital en 2025, un 228% interanual. Las alertas de este año hablan sobre todo de bancos, pero el método sirve igual contra una tienda, una clínica o un distribuidor: un perfil parecido, un número nuevo, una cuenta para pagar.

La cifra sobre Venezuela aparece en el artículo de Bloomberg Línea del 8 de mayo de 2026.
https://www.bloomberglinea.com/tecnologia/de-venezuela-a-el-salvador-los-paises-de-latam-donde-mas-aumento-el-fraude-digital/

Publica Reglas que Tus Clientes Puedan Comprobar

Según reseñó El Diario en abril, el Banco de Venezuela ha reiterado que sus comunicaciones oficiales no incluyen enlaces externos para verificar información. Es una regla corta que cualquier cliente puede aplicar. Un negocio puede publicar las suyas en una página de canales oficiales,

dentro de un dominio que controla, y hacer que todo apunte ahí: la biografía de cada red, la firma del correo, las respuestas automáticas de WhatsApp, las facturas y el empaque. Esa página debe leerse en un minuto y caber en la pantalla de un teléfono.

- Escribe los números de teléfono y de WhatsApp, el usuario exacto de cada red social y el correo de contacto, y verifica que coincidan con los que usas de verdad.
- Indica la razón social y el RIF a cuyo nombre recibes pagos, con las cuentas y los datos de pago móvil vigentes. Si cambias una cuenta, actualiza primero esta página.
- Di lo que nunca vas a pedir: códigos recibidos por SMS, contraseñas, pagos a cuentas que no estén en esta página o entrar a enlaces de otros dominios.
- Explica cómo reportar un perfil o un mensaje falso, quién recibe el reporte y en cuánto tiempo respondes.
- Muestra la fecha de la última revisión y actualiza la página cuando cambie un número, una cuenta o una persona del equipo.

Tu Catálogo No Debería Vivir Solo en un Perfil

El segundo riesgo es perder el perfil. El 15 de agosto, el Sindicato Nacional de Trabajadores de la Prensa (SNTP) informó que la cuenta de Instagram de El Nacional seguía suspendida tras denuncias fraudulentas por supuestas infracciones de derechos de autor, y que otros medios habían sufrido la eliminación de contenidos o la suspensión de cuentas por denuncias que el gremio calificó de falsas. En marzo, Meta anunció que en los próximos años usará IA más avanzada para aplicar sus normas, a medida que supere a sus métodos actuales, y que dependerá menos de proveedores externos; según la empresa, las personas seguirán teniendo un papel clave en las apelaciones por cuentas inhabilitadas.

El reporte del SNTP lo recogió El Diario el 15 de agosto de 2026.
https://eldiario.com/2026/08/15/sntp-denuncias-falsas-medios/

Esos casos son de medios, no de comercios, y no conocemos una cifra pública de negocios venezolanos suspendidos. Aun así, si los precios, las fotos y el contacto existen solo dentro de un perfil, perderlo deja al cliente sin dónde comprobar nada. Guarda fuera de la plataforma las fotos originales y las descripciones, con un enlace estable por producto en tu dominio. Lleva en un sistema propio la lista de clientes que aceptaron recibir novedades. Y deja escrito qué publicarás, y en qué canal, si la cuenta cae un viernes en la noche.

Cómo lo Resuelve la Página Web Anti-Apagón

Empezamos con un inventario de canales: cada número, usuario, correo y cuenta de pago, quién lo

administra y dónde aparece. Con eso redactamos la página de canales oficiales y la lista de lo que el negocio nunca pedirá, en una dirección corta y fácil de dictar. El catálogo vive en el sitio, con precio, fecha de actualización, disponibilidad y un botón al WhatsApp oficial; las redes enlazan a cada producto. El sitio se instala en el teléfono como aplicación web (PWA) y guarda esa página y el catálogo para consultarlos con mala conexión o sin ella. El flujo de pago acordado muestra las mismas cuentas que la página oficial. Añadimos un formulario de reporte de suplantaciones que llega a una persona con nombre.

> *Una página oficial ayuda a tus clientes a verificar, pero no impide que alguien cree perfiles o dominios falsos. Retirar una suplantación o restablecer una cuenta suspendida depende de cada plataforma, y ningún sitio web garantiza esa decisión. Las cifras citadas pertenecen a sus autores.*

Una Comprobación Concreta

Usa un teléfono en el que no tengas abiertas las cuentas del negocio. Entra a cada uno de tus perfiles públicos, sigue el enlace de la biografía y comprueba que lleva a tu propio dominio y muestra los mismos números y cuentas de pago que tus otros canales. Después busca en cada red el nombre del negocio y sus errores de escritura más comunes, y anota los perfiles que usan tu nombre, tu logo o tus fotos sin que los controles. No les escribas ni abras sus enlaces. Repórtalos con el procedimiento de cada plataforma: en Facebook, la opción para reportar el perfil o la página está en el menú de opciones (los tres puntos), y Facebook también recibe estos reportes de personas sin cuenta. Anota la fecha y el resultado para repetir la búsqueda el mes siguiente.

Documentación de apoyo: Instrucciones de Facebook para reportar un perfil o una página que se hace pasar por ti.
https://www.facebook.com/help/174210519303259

Para seguir leyendo: Tu Dominio No Debería Depender de un Correo Ajeno.
https://systems.kavaliero.com/blog/tu-dominio-no-deberia-depender-de-un-correo-ajeno

Si necesitas ayuda con este trabajo, consulta el alcance de Página Web Anti-Apagón.
https://systems.kavaliero.com/soluciones/web-anti-apagon