Endesa filtró tus datos en enero. La llamada "oficial" te llegará en abril (y no será de Endesa)

Por qué las grandes brechas de datos no terminan el día que salen en el telediario: empiezan ese día. Y cómo enseñar a tus padres a distinguir al operador real del estafador cuando ambos saben su DNI, su IBAN y su tarifa de luz.

Suena el teléfono en casa de tus padres. Al otro lado, una voz amable, profesional, sin prisa. Conoce su nombre completo. Menciona su DNI. Cita el IBAN donde domicilian la luz. Sabe qué tarifa tienen contratada con Endesa y cuánto pagaron el mes pasado. Dice que llama del departamento de facturación, que han detectado un cargo duplicado y que necesita confirmar unos datos para devolverles el dinero.

Tu padre no tiene motivo para dudar. La persona tiene **toda la información correcta**. Así que contesta.

Esa llamada no es de Endesa. Probablemente llegará entre abril y finales de 2026. Y no es una hipótesis: es la consecuencia matemática de algo que ya ocurrió en enero y que buena parte del país ha olvidado.

Lo que realmente pasó en enero (y por qué sigue pasando hoy)

El 12 de enero de 2026, Endesa Energía y su filial Energía XXI confirmaron que sufrieron un ciberataque grave en su plataforma comercial, donde un actor malicioso logró un acceso no autorizado y superó las medidas de seguridad de la compañía. La información sustraída no era trivial: nombres y apellidos, DNI, información de contacto, detalles contractuales y números de cuenta (IBAN).

Las contraseñas no cayeron. Pero eso es casi irrelevante para lo que viene después. El ciberdelincuente, identificado en foros de la dark web como "Spain", afirmaba haberse hecho con una base de datos de más de 1 TB que contenía 20 millones de registros de clientes, incluyendo datos financieros como IBAN, datos de facturación e historial de

cuentas y cambios; datos energéticos, como CUPS (identificador único de punto de suministro), contratos activos de luz y gas y datos regulatorios. Hasta el historial de incidencias.

Para quien diseña un engaño, esto no es una filtración: es un manual de instrucciones.

Endesa no ha sido la única este año. Hacienda, el Puerto de Vigo, la cadena de gimnasios Basic Fit e Inditex también han estado en el punto de mira durante 2026. Cada una de esas brechas alimenta el mismo circuito.

La mentira que nos han vendido: "la brecha ya está controlada"

Cuando una empresa comunica un ciberincidente, el titular suele transmitir la idea de cierre: *lo hemos detectado, lo hemos contenido, los datos afectados son X, gracias por su confianza*. El ciclo informativo dura tres días. A la semana siguiente, nadie habla ya del tema.

Pero desde la perspectiva del atacante, ese es precisamente el momento en que empieza el trabajo rentable. El ciclo real es otro, y conviene entenderlo bien:

Ataque → exfiltración → venta o publicación en foros clandestinos → uso en campañas dirigidas durante 12 a 24 meses.

Los datos robados no se queman en una sola operación. Se fragmentan, se cruzan con otras bases (las de la brecha de Hacienda, la de Basic Fit, la de Inditex) y se enriquecen. Un delincuente medianamente competente no te llamará mañana. Esperará a que olvides. A que la noticia desaparezca del titular. A que bajes la guardia. Hay que tener en cuenta que una información así puede ser reutilizada durante meses, e incluso años, para lanzar fraudes dirigidos.

Y hay un detalle que cambia completamente la conversación: el propio Instituto Nacional de Ciberseguridad (INCIBE) ya advirtió tras la brecha de que es posible que estas personas se vean afectadas por posibles campañas de phishing, smishing y llamadas telefónicas. Es decir, las autoridades ya saben que la ola viene. La cuestión es si tu familia lo sabe.

Por qué Energía XXI es el blanco perfecto (y por qué deberías leer esto pensando en tus padres)

Hay una razón muy concreta por la que este caso no se parece a una filtración genérica. Energía XXI es la comercializadora de referencia del mercado regulado de electricidad. Dicho sin jerga: es la empresa que suministra luz a quienes nunca han cambiado de compañía, a quienes tienen el precio PVPC, a las personas mayores que firmaron un contrato hace veinte años y no lo han tocado desde entonces.

Sus clientes no son perfiles con doble factor de autenticación y antivirus premium. Son, en muchos casos, las personas más vulnerables del ecosistema digital español. Y esos son precisamente los datos que hoy circulan por foros clandestinos.

Los atacantes lo saben. Y las autoridades de consumo ya han detectado intentos de estafa dirigidos específicamente a usuarios de Energía XXI, solicitando pagos urgentes o cambios de cuenta bancaria mediante llamadas telefónicas fraudulentas. En ciberseguridad aplicada esto tiene un nombre: **vishing** (phishing telefónico). Y cuando el estafador conoce de antemano tus datos reales, deja de ser una técnica torpe de marketing fraudulento para convertirse en algo muy parecido a la verdad.

La regla de oro que debes enseñar esta semana

La mayoría de los consejos de ciberseguridad que circulan por internet asumen que el receptor será capaz de detectar una incongruencia, un error ortográfico, un tono extraño. **Ese marco ya no funciona.** Cuando el atacante tiene tu DNI, tu IBAN y tu tarifa, no hay incongruencia que detectar. La guía mental tiene que cambiar.

Por eso, la única regla que realmente protege es estructural, no intuitiva:

Si alguien te llama sabiendo tus datos, cuelga y llama tú al número oficial.

No importa lo creíble que parezca. No importa lo amable que sea la voz. No importa que sepa el CUPS de tu suministro o el nombre de tu nieto. La regla no admite excepciones. Si la llamada es legítima, colgar no te cuesta nada: volverás a contactar y te atenderán igual. Si la llamada no es legítima, acabas de salvar la cuenta corriente.

Endesa, consciente de la situación, habilitó dos líneas oficiales de atención: el 800 760 366 para clientes de Endesa Energía y el 800 760 250 para los de Energía XXI. Guárdalos en la agenda del móvil de tus padres hoy, no mañana.

De la alerta puntual a la cultura familiar

Si algo me ha enseñado analizar este ecosistema durante los últimos años es que la ciberseguridad no se gana comprando productos ni leyendo listas. Se gana convirtiendo ciertas reflexiones en cultura doméstica y empresarial.

La brecha de Endesa no es un incidente aislado: es una muestra gratuita de cómo va a funcionar la ingeniería social durante los próximos años. Datos reales, cruzados con IA, utilizados en el momento exacto en que la víctima ya ha dejado de estar alerta. El ciberdelincuente de 2026 no hackea ordenadores: hackea la memoria de los humanos, que es mucho más corta.

La pregunta útil no es *"¿cómo evito que roben mis datos?"* —ese barco, para la mayoría, ya zarpó—. La pregunta útil es *"¿cómo reaccionará mi familia cuando los usen contra ella?"*.

Tu próximo paso (y son quince minutos reales)

Esta semana, haz estas tres cosas con tus padres, tus abuelos o cualquier persona mayor de tu entorno:

Primero, explícales de forma clara que **Endesa no llama para pedir confirmación de datos bancarios ni para devolver dinero**. Ni Endesa ni ninguna otra compañía seria. Si alguien lo hace, es una estafa. Punto.

Segundo, acordad juntos la **regla de oro**: cualquier llamada de una empresa se corta y se devuelve al número oficial guardado en la agenda. Guarda hoy mismo el 800 760 366 o el 800 760 250 en su teléfono, según corresponda.

Tercero, recuérdales algo que nadie les dijo en enero: **que sus datos estén filtrados no es culpa suya**, y por tanto tampoco lo será si reciben una llamada convincente. Desactiva la vergüenza antes de que aparezca. El miedo a quedar en ridículo es una de las razones principales por las que las personas mayores no cuentan que han caído en una estafa. Quítales esa carga por adelantado.

Si este análisis te ha sido útil, compártelo con alguien que no lo haya visto. En ciberseguridad aplicada, un artículo leído a tiempo vale más que mil antivirus instalados tarde. Visita el blog para más recursos gratuitos sobre ingeniería social, brechas de datos y cultura digital aplicada a familias y pymes.

Etiquetas: filtración Endesa 2026, estafas telefónicas mayores, phishing dirigido España, ingeniería social familia, ciberseguridad pymes, vishing Endesa, protección datos padres, brechas de datos España.