Los 5 ciberataques que debes conocer en 2026

Los ciberataques de 2026 no buscan empresas grandes ni sistemas complejos. Te buscan a ti. Descubre los cinco tipos de ataque que más están creciendo este año, cómo llegan y qué puedes hacer hoy mismo para no caer.

Explicados sin tecnicismos: qué son, cómo llegan y qué puedes hacer hoy para proteger tu familia y tu negocio.

Puede que creas que esto no va contigo. Que los ciberataques son cosa de grandes empresas, de bancos o de gobiernos. Pero la realidad en 2026 es justo la contraria: los criminales digitales han aprendido que atacar a personas normales, familias y pequeños negocios es más fácil, más barato y casi igual de rentable.

Lo más importante que debes saber es que estos ataques no dependen de errores técnicos. Dependen de la confianza. Tu confianza. Por eso, entender cómo funcionan —aunque sea de forma básica— es hoy una de las mejores cosas que puedes hacer por ti y por los tuyos.

Aquí tienes los cinco ataques que más están creciendo en 2026, explicados de forma sencilla y con lo que puedes hacer en cada caso.

1. Phishing con IA: el mensaje que parece real… y no lo es

El phishing es el intento de engañarte haciéndose pasar por alguien de confianza: tu banco, Hacienda, tu operadora de internet o incluso un compañero de trabajo. No es nuevo, pero en 2026 ha dado un salto enorme gracias a la inteligencia artificial.

Antes, estos mensajes tenían errores evidentes. Ahora los genera una IA que ha analizado cómo se comunica tu banco contigo, qué tono usa y qué información tuya es pública. El resultado es un correo o un SMS prácticamente indistinguible del original.

Qué hacer: Antes de hacer clic en cualquier enlace, entra directamente en la web oficial escribiéndola tú en el navegador. Y activa siempre la verificación en dos pasos en tus cuentas más importantes.

2. Ransomware: cuando te secuestran los archivos

Imagina que enciendes el ordenador de tu empresa y todos tus archivos están bloqueados. Aparece un mensaje: "Paga o los pierdes para siempre." Eso es un ransomware: un programa malicioso que cifra tus datos y pide un rescate económico para devolvértelos.

Lo que hace especialmente peligroso a este ataque en 2026 es que ya no solo bloquean: primero copian tus archivos y luego amenazan con publicarlos. Si tienes datos de clientes, facturas o información sensible, el daño puede ir mucho más allá de perder los ficheros.

Afecta tanto a familias (fotos, documentos personales) como a negocios de cualquier tamaño. Y lo peor: muchas veces entra por un simple correo con un archivo adjunto que alguien abrió sin sospechar nada.

Qué hacer: Haz copias de seguridad periódicas en un disco externo que no esté siempre conectado. Mantén el sistema operativo y las aplicaciones actualizadas. Y no abras archivos adjuntos que no esperabas recibir.

3. Deepfakes: la voz y la cara de alguien que no está ahí

Este es el ataque que más impacta cuando la gente lo conoce por primera vez. Con solo unos segundos de audio o vídeo —los que cualquiera tiene colgados en redes sociales— la inteligencia artificial puede imitar de forma convincente la voz y el rostro de una persona real.

En empresas, se usa para llamar haciéndose pasar por el director general y pedir una transferencia urgente. En familias, para llamar como si fuera un hijo en apuros pidiendo dinero. El engaño es tan bueno que es muy difícil detectarlo en el momento.

Qué hacer: Acuerda una "palabra clave" de seguridad con tu familia o equipo para situaciones urgentes e inusuales. Si recibes una llamada extraña de alguien cercano, cuelga y llama tú directamente al número que tienes guardado.

4. Ataques a través de proveedores: el camino más fácil hacia ti

Los criminales son estratégicos: si quieren atacar a una empresa grande con buena seguridad, no van de frente. Buscan a uno de sus proveedores más pequeños —una gestoría, una empresa de limpieza, una agencia de marketing— que tenga acceso a sus sistemas y que probablemente tenga menos defensas.

Desde ahí entran y se mueven sin que nadie lo note. Para las pymes esto es especialmente relevante: podéis ser tanto el objetivo final como la puerta de entrada involuntaria hacia uno de vuestros clientes.

Qué hacer: Revisa qué accesos tienes dados a empresas externas y asegúrate de que solo tienen permiso para lo estrictamente necesario. Si un proveedor no necesita acceso continuo, retíralo cuando acabe el trabajo.

5. Ingeniería social con IA: te conocen antes de escribirte

La ingeniería social es el arte de manipular a las personas para que hagan algo que no deberían: entregar una contraseña, hacer una transferencia, abrir un archivo. No es hackear ordenadores; es hackear personas.

Lo que ha cambiado en 2026 es que la IA puede analizar tu perfil público —tus publicaciones, tu empresa, tus horarios, tus intereses— y construir un ataque personalizado antes de contactar contigo. Saben tu nombre, conocen tu empresa, mencionan cosas reales de tu vida. No parece un engaño porque parece que te conocen.

Qué hacer: Revisa qué información tuya es pública en redes sociales y ajusta tu privacidad. Ante cualquier solicitud inusual —aunque parezca legítima—, verifica por otro canal antes de actuar.

Lo que tienen en común todos estos ataques

Fíjate en algo: ninguno de estos cinco ataques funciona porque tú seas descuidado o poco inteligente. Funcionan porque están diseñados para explotar la confianza, la urgencia y las emociones. Nadie está a salvo por defecto, y eso no es alarmismo: es la realidad del ecosistema digital en 2026.

La buena noticia es que la mayoría se pueden prevenir con tres cosas muy concretas: información (saber que existen), protocolos (tener una forma de verificar antes de actuar) y cultura (hablar de esto con tu familia y tu equipo). Ninguna de las tres requiere ser experto en tecnología.

Tu próximo paso (y son solo 20 minutos)

Hoy mismo puedes hacer tres cosas: activar la verificación en dos pasos en tu correo y tu banco, acordar una palabra clave de seguridad con tu familia para llamadas de emergencia, y revisar los accesos externos que tienes en tu empresa o en tus cuentas personales.

Si este artículo te ha sido útil, compártelo. Una persona informada es una persona más difícil de engañar, y eso beneficia a todos. Visita el blog para acceder a más recursos gratuitos sobre seguridad digital aplicada.

Isaac Ruiz Romero.