5 Ciberataques que Están Ocurriendo Ahora Mismo

DESCRIPCIÓN SEO: Descubre los 5 ciberataques más activos en febrero 2026 con ejemplos reales. Protege tu familia y empresa con pasos concretos. *(155 caracteres)*

Las amenazas reales de febrero de 2026 que afectan a familias, autónomos y empresas — explicadas sin tecnicismos.

Cada semana, miles de familias y negocios en España son víctimas de ataques digitales que no aparecen en los titulares. Ataques que no requieren que seas descuidado, que no dependen de que uses mal la tecnología. Solo necesitan que confíes. Y en febrero de 2026, ese ecosistema de amenazas ha dado un salto que merece atención inmediata.

Esta semana, los equipos de ciberseguridad de todo el mundo han publicado alertas sobre cinco vulnerabilidades y campañas activas que afectan directamente a usuarios corrientes, autónomos y pequeñas empresas. No son hipótesis. Están ocurriendo ahora mismo.

El problema no es la tecnología. El problema es que nadie te había explicado esto en un idioma que entendieras.

Aquí lo tienes.

1. Las Estafas del iPhone 17: Phishing en su Punto Álgido

Con el ciclo de post-lanzamiento del iPhone 17, los delincuentes digitales han activado una maquinaria de engaño que lleva semanas en marcha y que en febrero ha alcanzado su máxima intensidad. La mecánica es conocida pero la ejecución es cada vez más sofisticada: anuncios en redes sociales, correos electrónicos y SMS que prometen descuentos imposibles, sorteos exclusivos o acceso anticipado a promociones. Todo falso.

Lo que distingue estas campañas de las antiguas estafas por correo es el nivel de personalización. Los mensajes están redactados en un español impecable, imitan a la perfección las comunicaciones de Apple o de operadoras de telefonía, y dirigen a la víctima a páginas web que son copias visuales casi perfectas de las originales. El objetivo final es siempre el mismo: robar tus credenciales de iCloud y los datos de tu tarjeta bancaria.

El impacto real es doble. Quien pierde sus credenciales de iCloud no solo pierde acceso a sus fotos y documentos: entrega el control de su identidad digital a personas que pueden usarla para compras fraudulentas, suplantar su identidad ante terceros o incluso bloquear el dispositivo exigiendo un rescate.

✅ **Qué hacer:** Nunca accedas a ofertas de Apple desde un enlace recibido por correo o SMS. Ve siempre directamente a apple.com escribiéndolo tú en el navegador. Activa la verificación en dos pasos en tu ID de Apple hoy mismo.

2. Espionaje en Máquinas Virtuales de Dell: La Amenaza Invisible

El 18 de febrero de 2026, varios equipos de investigación publicaron información detallada sobre cómo el grupo de amenazas avanzadas conocido como UNC6201 ha logrado comprometer entornos de virtualización de Dell. Para quien no esté familiarizado con el concepto: una máquina virtual es como un ordenador dentro de un ordenador, un entorno supuestamente aislado que las empresas usan para separar sistemas y proteger datos críticos.

El ataque explota fallos en el firmware de estos entornos para saltar de la máquina virtual aislada al resto de la red corporativa sin dejar rastro. Es como si alguien encontrara un túnel secreto dentro de una caja fuerte. Las implicaciones son graves: una vez dentro de la red, los atacantes pueden moverse lateralmente durante semanas o meses antes de ser detectados, extrayendo propiedad intelectual, datos de clientes y credenciales de acceso.

Aunque este tipo de ataque se asocia con grandes corporaciones, el vector de entrada suele ser una empresa más pequeña del ecosistema: un proveedor, una consultora, una empresa de servicios que tiene acceso a los sistemas del cliente grande y que no ha aplicado las actualizaciones de seguridad correspondientes.

✅ **Qué hacer:** Si tu empresa utiliza entornos virtualizados de Dell, contacta con tu responsable IT o proveedor de servicios para verificar que los parches publicados esta semana han sido aplicados. Si eres pyme y no tienes a nadie en este rol, es el momento de buscar asesoramiento externo.

3. Vulnerabilidades Críticas en Fortinet: La Puerta de Entrada al Teletrabajo

Fortinet es uno de los proveedores de seguridad más utilizados por empresas medianas y pymes en España. Sus dispositivos VPN y sus firewalls protegen el acceso remoto de miles de trabajadores que operan desde casa o en movilidad. Esta semana, el INCIBE y varios boletines de seguridad internacionales han revalidado alertas sobre fallos graves que afectan a versiones no actualizadas de estos sistemas.

El fallo es técnicamente sencillo de entender en sus consecuencias: un atacante que conozca la vulnerabilidad puede acceder a la red corporativa sin necesidad de usuario ni contraseña. No necesita engañar a nadie. Solo necesita que el dispositivo no esté actualizado. Y la realidad es que en muchas empresas, los dispositivos de seguridad perimetral se instalan, se configuran y después se olvidan durante meses o años.

Las consecuencias de una intrusión por esta vía son diversas: desde el robo silencioso de información hasta el despliegue de ransomware que paralice toda la operativa de la empresa. Y lo más preocupante es que este tipo de acceso es difícil de detectar sin monitorización activa.

✅ **Qué hacer:** Consulta con tu proveedor de IT si los dispositivos Fortinet de tu empresa están actualizados. No lo dejes para la próxima revisión. Esta semana, este fallo está siendo activamente explotado.

4. ClickFix en España: El Virus que Tú Mismo Instalas

España continúa siendo uno de los países más atacados de Europa, con una media que supera los 1.800 ataques semanales a organizaciones según datos actualizados a principios de 2026. Entre las técnicas más activas en este momento destaca ClickFix, una campaña de ingeniería social especialmente efectiva porque convierte al usuario en el ejecutor involuntario del ataque.

El mecanismo funciona así: navegas por una web cualquiera y aparece un mensaje de error que parece legítimo. Te dice que para solucionar el problema debes copiar un código y pegarlo en la terminal o en el ejecutor de comandos de tu sistema. Al hacerlo, no estás arreglando nada: estás instalando un programa que, en segundos, extrae todas las contraseñas guardadas en tu navegador, tus cookies de sesión y tus credenciales de acceso a plataformas de gestión, correo y banca.

La razón por la que este ataque funciona tan bien es que el mensaje de error imita el lenguaje técnico que realmente aparece en los sistemas, y porque la instrucción de copiar y pegar se presenta como una solución rápida. El instinto humano de resolver un problema de forma inmediata hace el resto.

Nadie con acceso legítimo a tu sistema te pedirá que copies y pegues un código para arreglar un error del navegador. Nunca. Sin excepción.

✅ **Qué hacer:** Advierte a todos los miembros de tu equipo y familia sobre esta técnica. Si aparece un mensaje de error con instrucciones de copiar y pegar código, cierra el navegador sin hacer nada más. Ante la duda, consulta con alguien de confianza antes de actuar.

5. Fallos en Firmware Festo: Cuando el Ciberataque Afecta al Mundo Físico

Este último punto merece especial atención porque ilustra hacia dónde se dirige la amenaza digital en los próximos años. Los equipos Festo son dispositivos industriales ampliamente utilizados en fábricas, plantas de energía y sistemas de producción. Vulnerabilidades en su firmware, que han vuelto a la primera línea informativa este mes por informes de explotación activa, permiten a un atacante tomar el control remoto de estos sistemas.

Las implicaciones van más allá de la empresa propietaria del dispositivo. Cuando un sistema industrial es comprometido, el impacto puede extenderse a la cadena de suministro: retrasos en la producción, alteraciones en el suministro de materias primas, y en escenarios extremos, riesgo de sabotaje físico que afecte a infraestructuras críticas.

Para la mayoría de las personas que leen este artículo, este punto puede parecer lejano. Pero la cadena de suministro digital está interconectada de formas que no siempre son visibles: el proveedor de un componente pequeño puede ser la puerta de entrada a un sistema mucho más grande. Las pymes industriales que dependen de este tipo de equipamiento deben estar especialmente atentas.

✅ **Qué hacer:** Si tu negocio opera con equipamiento industrial conectado a red, solicita a tu proveedor de mantenimiento que verifique el estado de actualización del firmware. Implementa segmentación de red para aislar los sistemas industriales del resto de la red corporativa.

Lo Que Une a Todos Estos Ataques: La Confianza como Vulnerabilidad

Observa el patrón. El phishing del iPhone 17 explota tu confianza en Apple. El ataque ClickFix explota tu confianza en los mensajes de error del sistema. Las vulnerabilidades de Fortinet explotan la confianza que depositas en que tus herramientas de seguridad están bien configuradas. El espionaje en máquinas virtuales explota la confianza entre empresas y proveedores.

En el ecosistema digital de 2026, la confianza es el recurso más valioso y el más explotado. Los atacantes han dejado de invertir principalmente en vulnerabilidades técnicas complejas porque resulta más eficiente explotar la confianza que las personas y organizaciones depositan en sistemas, marcas y procedimientos.

Esto tiene una consecuencia directa: la ciberseguridad ya no puede ser solo una cuestión técnica delegada al departamento de IT. Es una cuestión de cultura organizacional y familiar. Cada persona que entiende cómo funcionan estos ataques se convierte en una capa de defensa adicional. Y cada persona que no lo entiende es un vector de entrada potencial.

El arma más poderosa del cibercrimen en 2026 no es el código. Es tu confianza. Y la mejor defensa es la información.

Tu Plan de Acción Esta Semana

Las amenazas de esta semana son reales y activas. Estas son las acciones prioritarias, ordenadas por impacto:

- **Verifica que los dispositivos Fortinet de tu empresa están actualizados.** Esta semana, no el próximo mes.
- **Activa la verificación en dos pasos** en tu ID de Apple, tu correo y tu banca online.
- **Habla con tu equipo (o tu familia) sobre la técnica ClickFix.** Muéstrales este artículo.
- **Revisa qué proveedores externos tienen acceso a tus sistemas** y retira permisos que ya no sean necesarios.
- **Si tienes equipamiento industrial conectado**, contacta con tu proveedor de mantenimiento esta semana.

Isaac Ruiz Romero.