ILUSTRACIÓN ADOBE STOCK

¿Y si te espían con la cámara de tu propio móvil?

Se llama 'camfecting' y hay señales que te pueden poner sobreaviso

J. C. CASTILLO

Una nueva palabra se ha colado en el diccionario de anglicismos relacionados con el segmento tecnológico: 'camfecting'. Llevamos años debatiendo sobre la posibilidad de que los dispositivos inteligentes nos escuchen para desplegar inserciones publicitarias relacionadas con nuestros intereses (sin que existan aún pruebas), pero no solemos reparar en las cámaras de los 'smartphones'. ¿Y si alguien las utilizara para espiarnos?

A esto último hace referencia el 'camfecting', que también se aplica a ordenadores, tabletas electrónicas y demás gadgets con ópticas. Según describe la firma de ciberseguridad McAfee, «esta técnica de 'hacking' permite a los delincuentes tomar el control de una cámara web (grabar vídeos y tomar fotografías) sin el conocimiento ni el consentimiento del usuario. Hablamos así de una grave violación de la privacidad que puede traer consecuencias devastadoras para las personas afectadas».

Existen, además, diferentes tipos de 'camfecting', según la metodología empleada para llevarlo a cabo. En la mayoría de casos, los 'hackers' utilizan programas maliciosos ('malware') enmascarados como aplicaciones legítimas y listos para descargar a través de páginas web fraudulentas. Al ejecutarse, infectan el dispositivo del usuario para hacerse con su webcam.

Los malhechores digitales también recurren a técnicas de suplantación ('phishing') para convencernos de que pinchemos en determinados enlaces y descarguemos dichos archivos, lo que deriva en el mismo resultado; pero es que igualmente pueden aprovecharse de los agujeros de seguridad presentes en aquellos dispositivos que ya no cuentan con soporte de su fabricante.

Si estás preguntándote para qué van a querer espiarte (con la vida tan rutinaria que llevas), la respuesta es que no todos los 'hackers' andan detrás de ministros o presidentes del Gobierno: a algunos les basta con atesorar grabaciones sensibles para chantajear o extorsionar a cualquiera. La modalidad más común es aquella en la que se nos amenaza con difundir imágenes de carácter íntimo en nuestras redes sociales si no apoquinamos cierta cantidad.

Además de la bomba atómica que esto último supone para nuestra salud mental, el 'camfecting' puede provocarnos graves consecuencias tanto legales como financieras. Y es que algunos ciberdelincuentes usan nuestras fotos y vídeos para confeccionar documentos de identificación ilegítimos con los que suplantarnos, siendo habituales los casos en que terceros solicitan préstamos bancarios a nombre de otra persona o estafan sin ton ni son en plataformas de compraventa.

Señales luminosas

Por fortuna, existen indicios de que alguien está espiándonos a través de la cámara de nuestro móvil. El primero y más evidente es el indicador luminoso de activación: si se enciende de forma intermitente o sin venir a cuento, podríamos estar siendo víctimas de 'camfecting'. Claro que no podemos descartar la posibilidad de que alguna aplicación esté accediendo a nuestra cámara en segundo plano, fruto de un error, ante lo cual conviene revisar los permisos concedidos a la misma dentro del aparato de ajustes.

Otras señales a considerar aluden al hecho de que nuestro gadget se encuentre comprometido, más que al comportamiento de la cámara en sí. Si la batería del móvil se agota más rápido de lo normal, el sistema operativo va a pedales sin razón aparente, o encontramos aplicaciones instaladas que no recordamos haber descargado, podríamos estar expuestos sin saberlo.

¿Qué hacer ante estas situaciones? Hay quien corta por lo sano tapando todas las cámaras con cinta aislante (o adquiriendo una funda provista de pestañas deslizantes, que ciegan la óptica físicamente), pero esto no es más que un parche. «Aunque el 'hacker' no pueda verte, sigues teniendo un problema. El mismo 'malware' que le permite controlar tu cámara, le da acceso a tu galería de fotos, tus mensajes y tu historial de navegación», explica Adrianus Warmenhoven, de la firma de ciberseguridad NordVPN.

Actualízate siempre

El experto recomienda instalar un antivirus especializado en la detección de 'malware', desconfiar de mensajes con enlaces sospechosos, evitar las redes wifi públicas (muy vulnerables) y descargar programas únicamente desde webs confiables. McAfee recalca también la importancia de mantener nuestros dispositivos actualizados a la última versión, lo que nos dará acceso a los parches de seguridad más recientes.

Si, pese a lo anterior, sospechamos que nos han 'hackeado' la webcam, debemos denunciarlo a las autoridades competentes para que investiguen la cuestión y eviten así la proliferación de víctimas. El Instituto Nacional de Ciberseguridad (INCIBE) ofrece un formulario en su sitio oficial, pero también podemos ponernos en contacto con la Policía Nacional y la Guardia Civil, quienes cuentan con equipos especializados en este tipo de amenazas.