Protección contra el spyware

ACTIVIST CHECKLIST

Última actualización **15 de octubre de 2026** Toma unos **30 minutos**

Esta copia se hizo el 14 de noviembre de 2026. Actualizamos nuestras guías seguido, a medida que cambian las amenazas y surgen mejores formas de protegerte. Para ver la versión más reciente, visita activistchecklist.org/es/spyware/

Traducido automáticamente: Esta página se tradujo automáticamente. Hasta ahora solo el 9% de la página fue revisado por una persona. El resto del texto puede tener errores. Ayúdanos a revisar esta traducción[1].

El spyware es software que infecta tu dispositivo para espiarte y robar tus datos sin que lo sepas o lo autorices. Los celulares son los dispositivos más atacados porque registran datos detallados de ubicación, códigos de autenticación de dos factores (2FA) y una gran cantidad de otra información personal, pero las laptops y otros dispositivos también pueden ser blanco de ataques.

El spyware puede extraer tus mensajes privados (incluso en aplicaciones de mensajería cifrada como Signal), acceder a tus códigos 2FA, monitorear tus conversaciones, rastrear tu ubicación en tiempo real e incluso encender tu cámara o micrófono sin que te des cuenta. Todos esos datos se envían a quien controla el spyware. Es como si estuvieran mirando sobre tu hombro mientras usas tu celular.

El spyware lo crean y venden empresas privadas a los gobiernos. No solo se usa contra personas criminales, sino también contra activistas, periodistas y abogados. Más recientemente, ICE ha comprado acceso a herramientas de spyware[2].

Los dos programas de spyware móvil más conocidos son Pegasus (de NSO Group) y Graphite (de Paragon Solutions). Ambas empresas fueron fundadas por ejecutivos que trabajaban para la Unidad 8200, el equivalente israelí de la NSA en Estados Unidos. Pero todo el tiempo se descubre spyware[3] más nuevo[4], y el spyware es solo una parte de un mundo más amplio: el del "malware " y el "stalkerware", que también usan los gobiernos opresores y las parejas abusivas para silenciar a la gente. El spyware puede incluso colarse a través de anuncios comunes en línea[5], sin que tengas que hacer clic.

¿Qué tan probable es que yo sea blanco de spyware?

Aunque los gobiernos dicen usar spyware solo contra personas criminales, hay muchos casos documentados en que se ha usado contra activistas políticos, periodistas y abogados:

- Organizadores y activistas de alto perfil (en Cataluña[6])
- Abogados de derechos humanos (en México[7])
- Periodistas de investigación (Ver Forbidden Stories[8] y Amnistía Internacional[9])
- También hemos visto casos en que familiares de las personas atacadas tuvieron sus dispositivos infectados con spyware. (Ver Citizen Lab[10])

A los gobiernos, desplegar spyware como Pegasus y Graphite les cuesta **decenas o cientos de miles** de dólares. **Por lo tanto, la gran mayoría de activistas NO van a ser blanco de spyware y se beneficiarían más de protegerse contra otras amenazas[11].**

Sugerimos que empieces con nuestra Lista esencial de seguridad[11] y luego vuelvas a esta guía. Esa guía te ayudará a protegerte contra tecnologías de vigilancia más baratas de desplegar, como el rastreo de ubicación o el software para abrir celulares que los cops pueden usar tras incautar tu dispositivo.

A medida que políticos represivos siguen empujando a Estados Unidos hacia el autoritarismo, debemos esperar que el spyware sofisticado se use más ampliamente contra activistas.

La buena noticia: los pasos que debes tomar para protegerte del spyware y el stalkerware también te ayudarán a protegerte de otros tipos de ataques que son más probables, así que vale la pena completarlos de todos modos.

> **No entres en pánico:** Es fácil leer sobre estas herramientas avanzadas de hackeo y preocuparse mucho. La mayoría de activistas no van a ser blanco de spyware. Los autoritarios quieren que creamos que son todopoderosos y que pueden ver todo lo que hacemos. Con unos pocos pasos simples podemos hacer que sea muy costoso, y políticamente riesgoso, que nos vigilen.

Protecciones básicas

TODO EL MUNDO Esta sección es para cualquier persona que haga trabajo de activismo o incidencia.

Completa nuestra lista de Conceptos básicos de seguridad digital

Esta guía cubre otros pasos importantes para protegerte del doxxing, como contraseñas, permisos de ubicación en apps y actualizaciones de software.

Si te preocupa el doxxing, es buena idea completar los pasos de nuestra lista de Conceptos básicos de seguridad digital →[11]

Muchos de estos pasos te protegerán si alguien intenta acceder a tus cuentas o dispositivos cuando eres blanco de doxxing.

Estos puntos de la lista de Conceptos básicos son especialmente importantes:

- **Desactiva el rastreo de ubicación** en la mayoría de las apps
- **Instala las últimas actualizaciones de software** en tu computadora, teléfono y apps
- Usa un **gestor de contraseñas**
- **Cambia tus contraseñas actuales** si son débiles o las reutilizas en varios sitios.
- Activa la **autenticación de dos factores** en tus cuentas importantes
- No hagas clic en **enlaces sospechosos**

Mantén tu teléfono (y laptop) actualizados con la última versión del sistema operativo

Te protege de hackers, spyware y las herramientas que usa la policía para hackear teléfonos.

DO: Instala las actualizaciones apenas te lo pidan

DO NOT: Seguir presionando el botón de "actualizar más tarde"

Cada vez que sale una nueva actualización del sistema operativo, se están corrigiendo fallas de seguridad. Cada actualización que no has instalado representa una lista más larga de formas en que la policía puede hackear tu dispositivo. Piénsalo como un edificio grande con cada vez más puertas sin llave.

Si tu sistema operativo no está actualizado, muchas de las otras recomendaciones de esta guía no protegerán tus datos.

Empieza por tu teléfono. Si estás haciendo algo de mayor riesgo, asegúrate de actualizar todos tus dispositivos.

CÓMO HACER LAS ACTUALIZACIONES

Como las actualizaciones de seguridad son tan importantes, **diseñamos una herramienta que te guía paso a paso**.

Revisa las actualizaciones de tu teléfono y computadora →

CÓMO HACER LAS ACTUALIZACIONES MANUALMENTE

Si prefieres hacer las actualizaciones manualmente, aquí te explicamos cómo hacerlo en cada dispositivo:

Haz clic para ver los pasos manuales

iPhone

1. **Verifica que tu dispositivo aún tenga soporte:** Revisa si tu iPhone aún tiene soporte[12]
2. **Sistema operativo:** Ajustes → **General** → **Actualización de software**
3. Las **apps** están configuradas para actualizarse automáticamente por defecto. Para verificarlo, ve a **Ajustes** → **Apps** → **App Store** y asegúrate de que **Actualizaciones de apps** esté activado.

Mac

1. **Verifica que tu dispositivo aún tenga soporte:** Revisa si tu Mac aún tiene soporte[12]
2. **Sistema operativo:** Menú Apple → **Ajustes del Sistema** → **General** → **Actualización de software**
3. **Apps instaladas desde la Mac App Store:** Estas apps están configuradas para actualizarse automáticamente por defecto. Para verificarlo, abre la **App Store**, ve a **App Store** → **Ajustes** y asegúrate de que **Actualizaciones automáticas** esté activado.
4. **Otras apps:** Busca actualizaciones desde la barra de menú superior → Haz clic en el nombre de la app → Haz clic en **Buscar actualizaciones** o **Acerca de [NOMBRE DE LA APP]**, o revisa en **Ajustes...**. Si no ves la opción de actualizar, puede que esté configurada para actualizarse automáticamente en segundo plano.

Android

1. **Verifica que tu dispositivo aún tenga soporte:** Revisa si tu Android aún tiene soporte[12]
2. **Sistema operativo:** Ajustes → **Sistema** → **Actualización del sistema** (puede variar según el fabricante)
3. Las **apps** de Google Play Store están configuradas para actualizarse automáticamente por defecto. Para verificarlo, abre **Play Store**, toca el ícono de tu perfil y ve a **Ajustes** → **Preferencias de red** → **Actualizar apps automáticamente**.

Windows

1. **Actualiza tu sistema:** Inicio → **Configuración** → **Actualización y seguridad** → **Windows Update**
2. **Verifica que tu dispositivo aún tenga soporte:** Revisa si tu equipo con Windows aún tiene soporte[12]
3. **Apps de la Microsoft Store:** Asegúrate de activar las actualizaciones automáticas[13] (activadas por defecto).
4. **Otras apps:** Busca actualizaciones en la barra de menú → **Ayuda** → **Buscar actualizaciones**, o busca **Actualizaciones** o **Acerca de** en la configuración de la app.

☐ Activa el Modo Aislamiento (iPhone) o Protección Avanzada (Google y Android)

El spyware es un tipo de ataque avanzado que aprovecha vulnerabilidades sofisticadas en nuestros dispositivos. En respuesta, Apple y Google han creado un modo de seguridad avanzado que ofrece mayor protección contra el spyware.

En los iPhone se llama **Modo Aislamiento**[14] y en Android se llama **Programa de Protección Avanzada**[15]. (También puedes activar el Programa de Protección Avanzada solo en tu cuenta de Google aunque no tengas un teléfono Android.)

No tenemos reportes de nadie que se haya infectado con spyware teniendo activado el Modo Aislamiento de Apple. La Protección Avanzada de Android es más reciente y todavía no se ha podido comprobar qué tan efectiva es.

Compromisos de uso: Ambas funciones implican sacrificar algunas funcionalidades. Mira la lista completa de compromisos[16]. Si te topas con problemas que no te funcionan, siempre puedes desactivar la función después.

CÓMO ACTIVAR EL MODO AISLAMIENTO EN IPHONE

IPHONE

Ajustes → **Privacidad y seguridad** → **Modo Aislamiento** → **Activar**

Esta función está disponible para iOS 16 en adelante.

CÓMO ACTIVAR LA PROTECCIÓN AVANZADA EN ANDROID

ANDROID

Ajustes → **Seguridad y privacidad** → en **Otros ajustes** toca **Protección Avanzada**

Nota: La ubicación de este ajuste puede variar entre dispositivos Android, así que te recomendamos buscar 'Protección Avanzada' en la barra de búsqueda de Ajustes.

Esta función está disponible para Android 16 en adelante.

Bloquea los anuncios en tu teléfono y computadora

Se ha distribuido spyware a través de anuncios comunes en línea, sin necesidad de hacer clic.

Citizen Lab descubrió[5] que se estaba distribuyendo spyware mediante anuncios dirigidos mostrados dentro de apps y sitios web de uso cotidiano. Con solo cargar el anuncio bastaba para infectar un dispositivo, aunque nunca lo vieras ni le hicieras clic.

Bloquear los anuncios cierra ese camino. También dificulta que los cops y los data brokers rastreen tu ubicación a través de las redes publicitarias[17].

CÓMO BLOQUEAR ANUNCIOS

- [ ] **Instala una VPN confiable con bloqueo de anuncios[17] en tu teléfono y mantenla activada.** Este es el paso más importante porque bloquea los anuncios dentro de tus apps, no solo en el navegador. En IVPN, activa **AntiTracker**. En Proton VPN, activa **NetShield** (solo en planes de pago). Mira cómo configurar una VPN[17].
- [ ] **Instala la misma VPN en tu computadora** y activa también ahí el bloqueo de anuncios.
- [ ] **Usa un navegador enfocado en la privacidad[11] que bloquee anuncios**, como Brave o Firefox con uBlock Origin[18]. Esto solo protege lo que haces en ese navegador.

Si no quieres usar una VPN, un servicio DNS con bloqueo de anuncios como AdGuard[19] puede bloquear los anuncios en todo tu teléfono. Mira DNS cifrado[17].

Desactiva el Advertising ID (que puede permitir que los cops rastreen tu ubicación)

Los cops usan herramientas que dependen de tu advertising ID para rastrearte

Sabemos que ICE y otras agencias policiales están usando herramientas de rastreo de ubicación[20] que dependen en parte del "ID de publicidad" que tu teléfono proporciona. Estas herramientas suelen usarse para reprimir movimientos sociales.

Los advertising IDs también se han usado para elegir blancos de spyware[21] que se entrega a través de anuncios.

En los iPhones, esta función está desactivada por defecto. En Android, viene activada por defecto y hay que desactivarla.

CÓMO DESACTIVAR EL ID DE PUBLICIDAD

IPHONE

Ajustes → **Privacidad y seguridad** → **Seguimiento** → **Desactivar el seguimiento de apps**

Por defecto, los iPhones ya tienen esta opción desactivada. Pero puedes revisarlo para asegurarte.

ANDROID

Ajustes → Toca el ícono de búsqueda y busca "anuncios" o "publicidad" → Toca **Eliminar ID de publicidad**

Esta opción aparece en lugares distintos según el teléfono, así que lo más fácil es buscarla.

Activa la Protección Avanzada de Datos de iCloud (iPhone) o el Programa de Protección Avanzada de Google

Apple, Google y otros servicios ofrecen funciones de seguridad adicionales para protegerte de ataques dirigidos a tus cuentas y datos. Estas protegen tus cuentas en línea con cada empresa, no el dispositivo en sí.

La Protección de datos avanzada de Apple activa el cifrado de extremo a extremo para la mayor parte de tu contenido.

CÓMO ACTIVAR LA PROTECCIÓN AVANZADA EN TUS CUENTAS DE CORREO/NUBE

Protege tus datos:

- Protección de Datos Avanzada de iCloud[22] - Activa el cifrado de extremo a extremo para casi todos los datos guardados en iCloud, protegiendo tu información frente a órdenes judiciales del gobierno. Asegúrate de guardar la clave de recuperación en un lugar muy seguro (como un gestor de contraseñas[11]).

Protege tu cuenta:

- Programa de Protección Avanzada de Google[23] - Ayuda a proteger tu cuenta contra phishing y accesos no autorizados.
- Account Guard de Microsoft[24]
- Proton Sentinel[25]

No hagas clic en enlaces sospechosos

Puedes protegerte del spyware si tienes cuidado con lo que abres

El spyware[21] suele llegar a través de un mensaje de texto o correo con un enlace hecho a tu medida, diseñado para que te resulte imposible ignorarlo. No son spam aleatorio: son ataques personalizados que aprovechan lo que más te importa.

CÓMO DETECTAR Y RESPONDER A ENLACES SOSPECHOSOS

Si tienes dudas: *¡No hagas clic en el enlace!*

1. En lugar de eso, contacta a quien te lo envió (ya sea una empresa o alguien conocido) por otro medio (llámale, usa otra app) para confirmar que realmente lo mandó. Tomarte 2 minutos para verificar siempre es mejor que hacer clic y comprometer tu dispositivo.
2. Si es una URL acortada como bit.ly o tinyurl.com, puedes usar ExpandURL.net[26] para ver la página de destino, pero esto no garantiza que la página no contenga spyware. Solo te ayuda a ver la URL real para que puedas evaluar mejor si confías en ella.
3. Para revisar si un enlace ya fue marcado como malicioso, puedes pegarlo en una base de datos de phishing y malware como VirusTotal[27] (propiedad de Google/Alphabet). Solo envía enlaces que sean públicos y no personales, ya que VirusTotal es un repositorio público que cualquiera puede consultar.

Señales de alerta a las que hay que prestar atención:

- **Mensajes de números que no reconoces:** A todes nos llegan seguido mensajes de servicios que no tenemos en nuestra libreta de contactos, así que puede costar distinguir si es un mensaje legítimo o no. Si es alguien que no está en tu libreta de contactos, tómalo con más cautela.
- **Urgencia o miedo**: "Tu cuenta será bloqueada", "Alerta de seguridad urgente", "Emergencia familiar"
- **Nombre de dominio desconocido:** Los mensajes de spyware suelen venir de dominios raros como `adsmetrics[.]co`
- **Demasiado personal**: Menciona tu activismo, eventos recientes a los que asististe o personas que conoces, con el fin de esquivar tu pensamiento crítico
- **Mensajes inesperados**: Un contacto te manda un enlace sin contexto, con frases raras o a una hora extraña (puede que su cuenta esté comprometida)
- **URLs acortadas**: `bit.ly`, `tinyurl.com` u otros acortadores de enlaces que ocultan el destino real
- **Errores de ortografía sutiles en la URL**: `goog1e.com` en lugar de `google.com`

Los mensajes con spyware pueden ser muy dirigidos. Aquí van algunos ejemplos reales de cómo se ha usado el spyware Pegasus:

> "Querida Carmen, mi hermano murió en un accidente, estoy devastado, te mando la información sobre el funeral, espero que puedas venir: [enlace de spyware]" (fuente[28])

> USEMBASSY.GOV/ DETECTAMOS UN PROBLEMA CON TU VISA, POR FAVOR ACUDE PRONTO A LA EMBAJADA. VER DETALLES [enlace de spyware] (fuente[28])

> LX 1955 BCN-ZRH 26Jun2020 - Haz clic en el enlace para recibir tu pase de abordar móvil [enlace de spyware] (fuente[29])

Ten en cuenta: Algún spyware se instala usando exploits que no requieren que hagas clic en ningún enlace ("exploits de cero clics" o "zero click exploits"). Estos pueden aparecer, por ejemplo, como llamadas perdidas en WhatsApp.

Protecciones avanzadas

AMENAZA MEDIA Esta sección es para ti si tienes un rol de liderazgo o haces un activismo que tiene más chance de ser atacado por el Estado o tu oposición.

Elimina todas las apps que puedas de tu teléfono o dispositivo

Si quieres ponerle más difícil a un ladrón entrar a tu casa, un paso fácil es reducir la cantidad de puertas. En tu dispositivo, cada app funciona como una "puerta" al mundo exterior, lo que te expone a un mayor riesgo de ataque. Si la app tiene un bug o una vulnerabilidad, puede hacer que todo tu dispositivo quede expuesto.

CÓMO ELIMINAR APPS

1. **Revisa todas las apps que tienes en tu teléfono** y computadora.
2. **Decide si realmente la necesitas.** A muchas apps puedes acceder fácilmente desde su sitio web. Suele ser un poco más incómodo, pero ganas más privacidad y seguridad a cambio.
3. **Desinstálala si es posible.** Si no estás seguro, prueba desinstalarla por una semana y mira si puedes arreglártelas sin ella. Siempre puedes reinstalarla después.

Ejemplos de apps que han sido usadas por spyware en el pasado:

- Apple HomeKit + FindMy + iMessage[30]
- Calendario de Apple[31]

Desactiva las vistas previas de enlaces en Signal y WhatsApp

Cuando incluyes un enlace en un mensaje, normalmente se genera una "vista previa del enlace". Aunque no lo veas, tu dispositivo está visitando esa página web para sacar la imagen de vista previa correcta. Si la página web es maliciosa, una persona atacante sofisticada puede identificar tu ubicación o, en casos extremos, instalar spyware en tu teléfono.

CÓMO DESACTIVAR LAS VISTAS PREVIAS DE ENLACES

- **Signal:** Abre Signal → Toca tu foto de perfil → **Ajustes** → **Chats** → **Desactiva Generar vistas previas de enlaces**
- **WhatsApp:** **Ajustes** → **Privacidad** → **Avanzado** → **Desactiva las vistas previas de enlaces**

Cubre la cámara frontal

Si ya te infectaron con spyware, pueden vigilarte en vivo a través de tu dispositivo, accediendo a la cámara y al micrófono. Para limitar lo que los espías pueden ver, es buena idea cubrir al menos tu cámara frontal.

CÓMO CUBRIR TU CÁMARA FRONTAL

1. Consigue una calcomanía que tenga suficiente pegamento para ser reutilizable. O considera este paquete de calcomanías de SLNT[32].
2. Ponla en tu teléfono y en tu laptop
3. Quítala temporalmente cuando necesites usar la cámara frontal, y recuerda volver a ponerla después.

Considera conseguir un teléfono secundario o desechable para el trabajo activista

Si encaja con tu forma de trabajar, considera usar un segundo teléfono o computadora solo para tu trabajo de mayor riesgo.

Revisa nuestra Lista de Verificación del Teléfono Secundario[33] para más información.

Si haces esto, asegúrate de mantener las precauciones de seguridad en todos los dispositivos. Aunque solo un dispositivo tenga comunicaciones o datos sensibles, ambos pueden ser blanco de spyware, ya que revelan tu ubicación y otra información personal que un atacante podría querer. Podrías considerar conseguir un teléfono compatible con **GrapheneOS**[34]. Es una versión de Android enfocada en la seguridad y la privacidad que funciona en los teléfonos Google Pixel.

Reinicia tu dispositivo con regularidad

La mayoría del spyware intenta ocultar su rastro al no escribir ningún archivo en tu dispositivo. Por eso, reiniciar tu dispositivo probablemente hará que el spyware se elimine por el momento. Dicho esto, si sigues siendo un objetivo, es probable que intenten reinfectar tu teléfono de inmediato. Algunas infecciones requieren que hagas clic en un enlace (o realices otra acción), pero otras ocurren sin ninguna interacción del usuario. Así que, aunque reiniciar tu teléfono con frecuencia puede ponerles las cosas más difíciles a quienes te atacan, no garantiza que estés libre de spyware.

Prueba de dispositivos

Si usas un iPhone, puedes hacer un análisis de spyware con iMazing[35]. Es gratis (no hagas clic en ninguno de los botones de "comprar"). Los usuarios técnicos también pueden usar el Mobile Verification Toolkit (MVT)[36] para hacer análisis forense detallado y consentido del dispositivo.

Sin embargo, detectar spyware en un dispositivo no es tarea fácil y no deberías confiarle tu celular a cualquier persona. Miembros de la sociedad civil en todo el mundo han recurrido a estas instituciones para analizar sus celulares y hacer análisis detallados con el apoyo de expertos:

- Citizen Lab[37] - las personas más expertas en análisis de spyware
- Access Now[38]
- Amnesty Security Lab[39]
- Constitutional Communications[40] - ayudan a llevar el análisis de spyware a más personas en comunidades activistas
- Electronic Frontier Foundation[41] - para gente en Estados Unidos

Cada organización tiene su propio proceso de verificación, y puede tomar un tiempo que respondan a tu solicitud mientras confirman todo de su lado.

Cómo detectar si podrías estar infectado

El spyware generalmente no presenta síntomas notorios e infecta *silenciosamente*. Sin embargo, algunas quejas comunes de personas atacadas con spyware a lo largo de los años incluyen:

- La batería del celular se descarga rápidamente
- Comportamiento sospechoso de ciertas aplicaciones
- Uso anormal de datos
- Recibir enlaces o adjuntos sospechosos

Si notas alguno de estos síntomas, no significa necesariamente que tu dispositivo haya sido hackeado con spyware. Te recomendamos contactar a alguna de las organizaciones enlazadas arriba para que analicen tu dispositivo.

El spyware es malware muy avanzado que un antivirus común **no va a detectar**. Recomendamos contactar a organizaciones expertas y confiables para que te ayuden a determinar si tu dispositivo muestra señales de haber sido comprometido (en el pasado o actualmente).

Apple y **WhatsApp** ahora notifican regularmente a sus usuarios cuando sospechan que sus dispositivos han sido atacados con spyware mercenario. Aquí tienes más info sobre las notificaciones de amenaza de Apple[42] y las notificaciones de amenaza de WhatsApp[43].

Aprende más

- Citizen Lab ha rastreado operaciones de Pegasus en 45 países[44]
- Forensic Architecture ha mapeado el costo humano de esas operaciones en su sitio, Digital Violence[45]

Relacionado: historia de cómo el gobierno de Estados Unidos ha comprometido la seguridad en internet:

- Microsoft le dio a la NSA acceso a mensajes cifrados[46] - The Guardian, 2013
- Revelado: cómo las agencias de espionaje de EE. UU. y el Reino Unido vulneran la privacidad y seguridad en internet[47] - The Guardian, 2013
- La N.S.A. es capaz de burlar las protecciones básicas de privacidad en la web[48] - The New York Times, 2013
- La NSA infectó 50,000 redes informáticas con software malicioso[49] - NRC, 2013
- Un contrato secreto vinculó a la NSA con un pionero de la industria de la seguridad[50] - Reuters, 2013
- N.S.A. idea una vía por radio para acceder a las computadoras[51] - The New York Times, 2014
- Cómo la NSA planea infectar "millones" de computadoras con malware[52] - The Intercept, 2014
- Ojos entrometidos: la guerra de la NSA contra la seguridad en internet[53] - Der Spiegel, 2014
- Un nuevo descubrimiento sobre la puerta trasera de Juniper genera más dudas sobre la empresa[54] - Wired, 2016
- La filtración de la NSA es real, los documentos de Snowden lo confirman[55] - The Intercept, 2016

Sigue aprendiendo con estas guías relacionadas

Defensa contra doxxing

Protégete del doxxing y del acoso en línea.

Planificación de emergencia

Arma una red de apoyo de emergencia en caso de que te detengan o te amenacen.

Póster "La poli en la puerta" 56

Enlaces

1. activistchecklist.org/es/contribute/
2. 404media.co/were-suing-ice-for-its-2-million-spyware-contract/
3. unwall.app/www.wired.com/story/coruna-iphone-hacking-toolkit-us-government/
4. unwall.app/www.wired.com/story/hundreds-of-millions-of-iphones-can-be-hacked-with-a-new-tool-found-in-the-wild/
5. citizenlab.ca/research/how-discover-tech-turned-targeted-ads-into-a-pipeline-for-spyware/
6. citizenlab.ca/research/catalangate-extensive-mercenary-spyware-operation-against-catalans-using-pegasus-candiru/
7. citizenlab.ca/research/lawyers-murdered-women-nso-group/
8. forbiddenstories.org/pegasus-the-new-global-weapon-for-silencing-journalists/
9. securitylab.amnesty.org/case-study-the-pegasus-project
10. citizenlab.ca/research/reckless-exploit-mexico-nso/
11. activistchecklist.org/es/essentials/
12. activistchecklist.org/es/updates/
13. support.microsoft.com/en-us/windows/turn-on-automatic-app-updates-70634d32-4657-dc76-632b-66048978e51b
14. support.apple.com/en-us/105120
15. landing.google.com/intl/en_us/advancedprotection/
16. activistchecklist.org/es/lockdown/
17. activistchecklist.org/es/vpn/
18. ublockorigin.com
19. adguard.com/en/welcome.html
20. 404media.co/inside-ices-tool-to-monitor-phones-in-entire-neighborhoods/
21. activistchecklist.org/es/spyware/
22. support.apple.com/es-es/108756
23. landing.google.com/advancedprotection/
24. accountguard.microsoft.com
25. proton.me/support/proton-sentinel
26. expandurl.net
27. virustotal.com/gui/home/url
28. citizenlab.ca/2017/06/reckless-exploit-mexico-nso/
29. citizenlab.ca/2022/04/catalangate-extensive-mercenary-spyware-operation-against-catalans-using-pegasus-candiru/
30. citizenlab.ca/2023/04/nso-groups-pegasus-spyware-returns-in-2022/
31. citizenlab.ca/2023/04/spyware-vendor-quadream-exploits-victims-customers/
32. slnt.com/products/webcam-cover
33. activistchecklist.org/es/secondary/
34. grapheneos.org
35. imazing.com/spyware-analyzer
36. github.com/mvt-project/mvt
37. citizenlab.ca/spyware-outreach/
38. accessnow.org/help/
39. securitylab.amnesty.org/get-help/
40. constitutionalcommunications.org
41. eff.org/about/contact
42. support.apple.com/en-us/102174
43. faq.whatsapp.com/641700318302674
44. citizenlab.ca/research/hide-and-seek-tracking-nso-groups-pegasus-spyware-to-operations-in-45-countries/
45. digitalviolence.org
46. theguardian.com/world/2013/jul/11/microsoft-nsa-collaboration-user-data
47. theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security
48. unwall.app/archive.nytimes.com/www.nytimes.com/interactive/2013/09/05/us/documents-reveal-nsa-campaign-against-encryption.html
49. nrc.nl/nieuws/2013/11/23/nsa-infected-50000-computer-networks-with-malicious-software-a1429487
50. reuters.com/article/us-usa-security-rsa-idUSBRE9BJ1C220131220
51. unwall.app/www.nytimes.com/2014/01/15/us/nsa-effort-pries-open-computers-not-connected-to-internet.html
52. theintercept.com/2014/03/12/nsa-plans-infect-millions-computers-malware/
53. spiegel.de/international/germany/inside-the-nsa-s-war-on-internet-security-a-1010361.html
54. unwall.app/www.wired.com/2016/01/new-discovery-around-juniper-backdoor-raises-more-questions-about-the-company/
55. theintercept.com/2016/08/19/the-nsa-was-hacked-snowden-documents-confirm/
56. activistchecklist.org/es/police/