AUTORIA

Amarelu y Martu Isla (Amartu)

AGRADECIMIENTOS

Muchas gracias a las compañeras de Navegando Libres, Fembloc, Luchadoras y Maria d'Ajuda por su tiempo y por compartir tantas ideas. Esperamos que este material sirva de devolución y esté a la altura de su tremendo trabajo.

Muchas gracias a la Rede Transfeminista de Cuidados Digitais por compartir su infraestructura digital.

Muchas gracias también a Ariel, Lux, Foz, Tes, Inés y todas las personas que tomaron su tiempo para revisar el contenido y darnos su feedback.

Muchas gracias al Center for Digital Resilience por confiar en nosotres para el desarrollo de este proyecto.

VERSION WEB Y DESCARGAS

es.celularhackeado.net (en Español)

pt.celularhackeado.net (en Portugués)

CONTACTO

amartu-zine@riseup.net

<TU PAREJA NO ES HACKER>

Parte 1: Desmitificando el hackeo de celulares

Licencia

36 https://labekka.red/licencia-f2f/

- No te creas todo lo que se dice en internet. Fíate solo de webs oficiales o recursos de confianza.
- Reduce el número de aplicaciones en tu dispositivo.
- Prueba a restaurar a valores de fábrica tu celular al menos una vez al año.

Sabemos que todos estos pasos pueden ser abrumantes, busca un lugar seguro, cómodo, tiempo, paciencia y personas de confianza que pueda acompañarte.

¡Hackea al patriarcado: fortalece tus conocimientos en tecnología! ¡ESTAMOS SEGURES DE QUE SABES MUCHO MÁS DE LO QUE PIENSAS!

Hoy en día los celulares son casi una extensión de nuestro cuerpo, de nuestros brazos: **¡Dediquemos el tiempo necesario a entenderlos, configurarlos y a que funcionen para nosotres!** Y recuerda también tener tiempos de descanso de la tecnología :)

Contenidos

Introducción

Al colaborar con líneas de ayuda feministas dedicadas a los cuidados digitales, notamos que existen muchos mitos en torno al tema de la invasión de celulares, lo que genera ideas erróneas que alimentan sentimientos de impotencia, angustia y paranoia entre personas que atraviesan situaciones de violencia. A partir de esta experiencia, desarrollamos un contenido que busca desmitificar estas creencias y ofrecer información accesible sobre hackeo y análisis de celulares, procurando un equilibrio entre la gravedad de los riesgos y un enfoque cuidadoso y realista. Esperamos que este material sea útil tanto para quienes enfrentan la violencia digital como para sus redes de apoyo y para las propias líneas de ayuda, que constantemente enfrentan y desmontan estos mitos.

Para producir este contenido, realizamos entrevistas con cuatro líneas de apoyo feministas en cuidados digitales: **Navegando Libres**, de Ecuador; **Luchadoras**, de México; **Maria d'Ajuda**, de Brasil; y **Fembloc**, de Cataluña. En estos encuentros conversamos sobre los mitos que cada línea identificaba, los motivos por los cuales exis-

5. **Revisa tus apps instaladas**, comprueba que sabes para qué es cada una, busca en internet el nombre de la aplicación si tienes dudas.

6. **Revisar el celular con un antivirus**, puedes usar Malwarebytes[33] (puedes usar la versión de prueba y luego desinstalar) o Koodous[34]. Evita otros antivirus y desinstala después de hacer la revisión[35].

7. **Comprueba que no tienes** activadas funcionalidades o apps de **control parental**.

8. **Comprueba la configuración de "Buscar mis dispositivos"**.

9. Haz un uso de la tecnología lo **más consciente y prudente posible**.

- Evita el caos, usa métodos o herramientas que te ayuden a ordenar, como un gestor de contraseñas.
- No le des a todo "ok" o "siguiente", sin leer.
- No instales apps de fuentes desconocidas o sin revisar bien si son lo que dicen ser.

33 https://www.malwarebytes.com/es/
34 https://koodous.com/product/koodous-mobile
35 Recuerda: el mejor antivirus eres tú.

3. **Organiza y fortalece tus contraseñas**:

- Elige un gestor de contraseñas con el que te sientas confortable (algunos recomendados son Bitwarden[29], KeePassXC[30], KeePassDX[31], 1Password[32]).
- Pon una contraseña diferente y fuerte para cada cuenta.
- Organiza las contraseñas en tu nuevo gestor de contraseñas.
- No las guardes en el navegador o el gestor de contraseñas de Google o iCloud.
- Activa una doble autenticación para todas las cuentas que consideres más importantes.

4. **Revisa tus configuraciones**:

- Reduce tus métodos de recuperación de cuentas a email o números de teléfono a los que tengas acceso constante. Ahí es donde llegarán las alertas en caso de intentos de recuperación de cuenta.
- Revisa las sesiones iniciadas. Cierra todas las sesiones que no reconozcas.

29 https://bitwarden.com/
30 https://keepassxc.org/
31 https://play.google.com/store/apps/details?id=com.kunzisoft.keepass.free&hl=es
32 https://1password.com/es

tían esos mitos, los imaginarios que los sostienen, y qué contenidos podrían ser útiles para ayudar a desmontarlos.

Finalmente, decidimos **organizar el contenido en dos partes distintos**, una dedicada a **desmitificar el hackeo de celulares** y otra enfocada en **desmitificar el análisis de celulares**, es decir, el análisis que se hace para detectar señales de hackeo.

El cuadernillo que tienes en tus manos es la parte 1, donde intentamos aclarar algunos conceptos, explicar las formas más comunes de intervenir un celular, cómo funciona realmente un software espía, qué síntomas pueden ser preocupantes y cuales no... entre otros contenidos que nos parecían relevantes para desmontar mitos sobre el hackeo de celulares y los supuestos hackers. También añadimos referencias de dónde buscar ayuda y recomendaciones básicas para que ¡hacker puedas ser tu!

Este fanzine nace como proyecto final de la Fellowship del Center for Digital Resilience de la que fuimos parte entre agosto de 2024 y julio 2025. Fue un trabajo a cuatro manos, con cuatro horas de diferencia ho-

raria, desde dos orillas muy alejadas del océano Atlántico, entre Río de Janeiro y las Islas Canarias.

En este material utilizamos lenguaje neutro y la letra "e" para referirnos a cualquier persona que pueda estar enfrentando una situación de violencia mediada por la tecnología. Esta es una apuesta feminista inclusiva hacia personas trans y no binarias. Esperamos que te sientas cómode al leerlo.

Esperamos que te guste y te sea útil ♥

Amarelu y Martu

10. Breves consejos para que le hacker seas tú

Sabemos que puedes estar en una situación muy estresante, angustiante y necesitas soluciones. Sin embargo, queremos avisarte de que, como casi todo en esta vida: ¡no hay soluciones mágicas!

Nuestros mejores consejos son:

1. **Busca apoyo emocional**, júntate con tus amigues y seres queridos.

2. **Trata de ordenar tu vida digital**:

- Lista tus cuentas de Google, iCloud o Microsoft.
- Lista otras cuentas de email (de yahoo, hotmail, etc).
- Lista tus redes sociales.
- Lista tus dispositivos (celulares, tablets, relojes, TV, computadores, etc).
- Identifica qué cuenta tienes configurada en cada dispositivo.
- Identifica los correos, números de teléfono u otros métodos de recuperación de las cuentas de redes sociales y correo.

Si necesitas atención en otros idiomas y territorios puedes consultar el índice de líneas de ayuda feminista: *feministhelplines.org.*

Además, si eres **activista, defensore de derechos humanos, periodista, abogade** y/o trabajas en temas sensibles por los que gobiernos u otras entidades puedan perseguirte, te recomendamos estas líneas de atención:

- Access Now[24], con soporte internacional: atención en 9 idiomas.
- SMEX[25], de Líbano: atención en inglés y árabe.
- Amnesty Tech[26], con soporte internacional.
- Front Line Defenders[27], con soporte internacional: atención en muchos idiomas.

Amnistía Internacional también ofrece una base de datos[28] donde puedes encontrar más organizaciones que pueden ayudarte, en otros idiomas y contextos.

24 https://www.accessnow.org/help-es/
25 https://smex.org/helpdesk/
26 https://securitylab.amnesty.org/es/get-help-digital-forensic-support/
27 https://www.frontlinedefenders.org/en/emergency-contact-human-rights-defenders
28 https://securitylab.amnesty.org/digital-resources/

1. ¿Me hackearon?

De repente tu celular empieza a comportarse de forma extraña. La batería se descarga demasiado rápido, las aplicaciones se traban sin explicación. Sientes que algo anda mal, como si, mágicamente, alguien estuviera leyendo tus pensamientos o siguiéndote a la distancia. Tu excompañere publica algo muy parecido a lo que acabas de comentar con una amiga. Una captura de pantalla que no recuerdas haber hecho aparece en tu galería. Y, como si fuera poco, una nueva sugerencia de contacto te resulta demasiado específica como para ser sólo una coincidencia. Son pequeñas cosas, desconectadas, pero que al sumarse te hacen preguntarte: "**¿Me hackearon?**"

No estás alucinando, estas cosas realmente pueden pasar. Pero es importante tener cautela: no siempre significan que te hackearon. A veces son fallas técnicas, errores del sistema, efectos de actualizaciones o del funcionamiento invasivo de los algoritmos. Sea como fuere, eso no disminuye la seriedad de lo que estás sintiendo. **La angustia es real. La duda es legítima**.

Esa duda no surge de la nada. Vivimos en un contexto de vigilancia constante, y eso, por sí sólo, ya puede generar incomodidad. Cuando hay un historial de violencia, amenazas o conflictos —ya sea en casa, en el trabajo o en una relación—, es común que el cuerpo entre en estado de alerta. Empezamos a prestar atención a cualquier comportamiento extraño del celular y estos problemas cotidianos pueden activar recuerdos, miedos y mecanismos de defensa.

La falta de conocimiento sobre cómo funcionan los sistemas también puede contribuir a esta situación. No siempre sabemos a qué tipo de datos realmente acceden las aplicaciones, o por qué ciertas cosas aparecen en la pantalla. Eso hace que los celulares se transformen en una fuente constante de inseguridad. **Cuando la tecnología parece incomprensible y misteriosa, también se vuelve amenazante**.

Además, el desconocimiento también provoca que, en una relación, generalmente las personas deleguen la tarea de configurar el celular, instalar aplicaciones, crear contraseñas y resolver problemas técnicos a la otra persona que "sabe más" de tecnología (generalmente un

lores de fábrica y no dejes tu cuenta de Google o Apple iniciada.

9. Dónde puedes buscar ayuda (trans)feminista

Estas son algunas líneas de ayuda feminista que te recomendamos:

- Maria d'Ajuda[19], de Brasil: atención en portugués y español.
- Navegando Libres[20], de Ecuador: atención en español.
- Luchadoras[21], de México: atención en español.
- Fembloc[22], de Cataluña (España): atención en español y catalán.
- Centro S.O.S. Digital de Internet Bolivia[23], de Bolivia: atención en español.

19 https://mariadajuda.org/index-es.html
20 https://navegandolibres.org/
21 https://luchadoras.mx/formulario/
22 https://fembloc.cat/
23 https://sosdigital.internetbolivia.org/

Al entregar tu celular a alguien, estás permitiendo que esa persona tenga acceso físico al dispositivo y, potencialmente, a tus datos, pudiendo acceder a información sensible como fotos, mensajes, aplicaciones bancarias, contraseñas y otros datos privados. Además, existe el riesgo de que esa misma persona instale aplicaciones maliciosas. También hay que desconfiar de promesas milagrosas y de personas alarmistas, especialmente cuando no hay transparencia sobre los métodos que pretenden utilizar. Corres el riesgo de pagar caro por servicios que no cumplen lo que prometen.

Si necesitas ayuda, busca espacios feministas y transfeministas, que sabrán brindarte apoyo más allá de los aspectos meramente técnicos. La mayoría de las veces, lo que realmente necesitamos es comprender mejor los dispositivos que utilizamos, ganando así más autonomía, tranquilidad y seguridad.

Si lo que necesitas es simplemente reparar algo que no está funcionando bien en tu celular, recuerda llevar siempre el dispositivo al servicio técnico de tu confianza lo más limpio posible, sin fotos ni documentos importantes o sensibles. Utiliza la opción de restaurar a los va-

hombre cis). Esto crea una dependencia que, al terminar la relación, puede transformarse en una vulnerabilidad. De ahí nace el mito de "**mi ex es hacker**": por saber un poco más o tener más familiaridad con los dispositivos, la persona parece tener poderes sobrenaturales sobre la tecnología. Y sobre ti.

***Sobre las palabras "hacker" y "hackear"**:*

Nos gustaría aclarar que no queremos contribuir a la connotación negativa de las palabras "hacker" o "hackear". Para nosotres, une hacker es una persona curiosa, con habilidades diversas (técnicas o no), que consigue subvertir los sistemas, las normas, los estándares. Sus propósitos pueden ser positivos en términos de justicia social, o todo lo contrario.

Invitamos a repensar la idea de "hacker" y "hackear" cómo algo más positivo, subversivo y creativo. Dejemos de contribuir a la idea de hacker como ese hombre-blanco-hetero-cis con capacidades técnicas extraordinarias. Ni estos seres tienen tantas capacidades ¡Ni nosotres tenemos tan pocas! ***¡Hackeemos estas ideas!***

2. ¡Tu cuenta, tu dispositivo y tu línea telefónica no son lo mismo!

Cuando sentimos que algo extraño está ocurriendo con nuestro celular, es común imaginar que el dispositivo fue hackeado, es decir, que el problema está en el aparato en sí. Pero, en realidad, existen diferentes capas que, si se ven comprometidas, pueden afectar nuestra privacidad y seguridad en el uso del teléfono móvil. Algunas de estas capas son: el dispositivo en sí y su sistema operativo, las cuentas vinculadas (como Google o Apple ID) y la línea telefónica. Cada una de ellas tiene sus propias características y consecuencias en caso de que alguien tome el control. Comprender estas diferencias ayuda a reconocer riesgos reales, evitar diagnósticos apresurados y buscar soluciones adecuadas a tus necesidades con mayor tranquilidad y autonomía.

Dispositivo (el celular)

Si el dispositivo está comprometido significa que algún software malicioso (*malware*) fue instalado en el sistema, generalmente con el objetivo de espiar, controlar, robar datos o dinero, o dañar el funcionamiento del

Es muy improbable / es lo menos común (aunque dependiendo de tú perfil, sí podría ocurrir)**:**

- **Tener un software espía altamente sofisticado** (como pegasus). Si NO eres periodista, abogada o activista trabajando en temas especialmente sensibles en tu región, es MUY probable que NO tengas un software espía de este tipo, ni que tu (ex)pareja lo pueda usar para vigilarte. Una persona individualmente no puede acceder al mercado de este tipo de tecnologías, solo se vende a gobiernos y tiene un coste de MILES de dólares[18].

8. Precauciones con supuestos hackers y servicios técnicos

Cuando surge la sospecha de que nuestro celular ha sido hackeado, es común que la angustia nos lleve a buscar soluciones inmediatas. En ese momento de vulnerabilidad, muchas personas terminan recurriendo a supuestos hackers o servicios técnicos poco confiables. El problema es que, en lugar de ayudar, estas alternativas pueden empeorar aún más la situación.

18 https://www.elnacional.cat/es/politica/precio-espionaje-pegasus-cuesta-pinchar-movil_760770_102.html

Sin embargo, si no autorizas la instalación de una fuente desconocidas y otras advertencias del sistema, difícilmente podrá acceder a los datos de tu celular.

- Si fuiste a instalar una aplicación confiable pero no la verificaste bien y resultó ser otra aplicación fraudulenta, podría ser una aplicación maliciosa que accediera a tus datos o añadiera publicidad invasiva. Revisa con atención cada aplicación antes de instalar. **No descargues o instales apps fuera Google Play o Apple Store a no ser que sepas MUY BIEN qué estas haciendo.**
- Si sufriste una estafa en la que alguien se hizo pasar por tu banco y otra compañía de tu confianza y te guió para instalar una aplicación fraudulenta, ahí si podría haber un acceso a los datos de tu celular.
- Si llevaste tu celular a un servicio técnico o alguna persona conocida que decía ser "hacker", al tener acceso al teléfono desbloqueado, pudieron ver todos tus datos e inclusos pudieron descargarlos o instalar apps o hacer nuevas configuraciones. Si necesitas reparar un celular llévalo vacío (valores de fábrica) y no dejes tu cuenta de Google o Apple iniciada.

aparato. Existen diferentes tipos de *malware*. Los más simples permiten un acceso o monitoreo limitado y, por lo general, requieren tener acceso físico al celular objetivo para poder instalarse. Los más sofisticados permiten un acceso amplio al dispositivo, pero su uso implica un alto costo, incluso político.

Cuenta vinculada (Google o Apple)

Significa que la cuenta de Google o Apple vinculada al dispositivo puede ser accedida sin necesidad de usar software espía o tener conocimientos técnicos muy avanzados. Basta con tener la contraseña de la cuenta, o acceso a algún dispositivo donde la cuenta esté activa. En contextos íntimos, por ejemplo, es muy común que parejas o familiares compartan contraseñas o mantengan dispositivos con múltiples cuentas de Google activas. Esto crea una vulnerabilidad significativa, ya que al tener acceso a la cuenta es posible explorar información sensible y realizar diversas acciones de distinto tipo, como veremos a continuación.

Con acceso a la cuenta Google, se puede:

→ Rastrear, bloquear o incluso borrar el contenido del celular de forma remota a través de "Encontrar mi dispositivo";

→ acceder al historial de lugares visitados (si está activado en la cuenta), mediante el "Historial de ubicaciones";

→ ver imágenes y videos almacenados en la nube con Google Fotos;

→ leer tus correos y archivos adjuntos mediante Gmail;

→ acceder a documentos y archivos guardados en Google Drive;

→ ver citas, recordatorios y lista de contactos mediante Calendario y Contactos;

→ acceder al historial de búsquedas y navegación (si está activado en la cuenta);

→ descargar una copia de todos los datos anteriores de una sola vez, usando Google Takeout; y

→ tener acceso a amplio rango de información relacionada con el uso del celular, como el uso de apps, rutinas y hábitos, y, en algunos casos, datos de salud, historial de llamadas y SMS, etc.

bién permite el borrado de datos del dispositivo y la localización de AirPods, AirTags y otros accesorios compatibles.

- Si tu (ex)pareja tuvo acceso físico a tu dispositivo y tiene algunos conocimientos de tecnología, pudo instalar alguna aplicación específica para monitorizar tu ubicación, acceder el micrófono, tomar fotos o ver la totalidad de la pantalla. La organización feminista *Echap* mantine un listado de aplicaciones que se pueden usar con este fin[14]. Estas aplicaciones pueden anunciarse por sus funcionalidades de control parental (la gran mayoría se anuncian así, por ejemplo, AirDroid Parental Control[15]), antirobo (como Cerberus[16]) o de acceso remoto a dispositivos para facilitar el soporte técnico (como AirMirror[17]).
- Si por error hiciste clic en algún enlace que simulaba ser confiable (SMS, DM en red social, email, etc), se podría haber descargado algún archivo malicioso.

14 https://github.com/AssoEchap/stalkerware-indicators?tab=readme-ov-file#stalkerware
15 https://play.google.com/store/apps/details?id=com.sand.airdroidkidp
16 https://www.cerberusapp.com/home/es
17 https://play.google.com/store/apps/details?id=com.sand.airmirror&hl=es

• **Instalaciones o configuraciones sospechosas después de llevar tu celular a un servicio técnico** o a alguien que decía que era "hacker", que puede implicar el acceso a tus datos por parte de estos servicios e incluso extorsión.

Por ejemplo:

• Si tu (ex)pareja tuvo acceso a tu celular y configuró Family Link[11] como si fueras su hije > lo más probable es que pueda ver tu ubicación e historial de ubicaciones (si tienes activada la ubicación), tus búsquedas en google y google maps y también bloquear tu celular o restringir contenidos o apps.

• Si tu (ex)pareja consiguió acceso a tu cuenta de Google o Apple puede iniciar las funcionalidades de "buscar mi dispositivo" (Buscar[12] en iOS y Buscar mi dispositivo[13] en Android) > si tienes la ubicación activada lo más probable es que pueda ver la ubicación del celular, sin embargo, cuando se active el teléfono emitirá un sonido y un aviso. Esta funcionalidad tam-

11 https://families.google/intl/es/familylink/
12 https://www.apple.com/es/icloud/find-my/
13 https://www.google.com/android/find/about

Con acceso a la cuenta de Apple, se puede:

→ Localizar, bloquear o borrar el dispositivo a través de "Buscar iPhone";

→ acceder a fotos y videos guardados en iCloud;

→ ver correos vinculados a iCloud Mail;

→ acceder a copias de seguridad del iPhone, que pueden incluir mensajes de iMessage, datos de apps e incluso de WhatsApp (si se hace copia de seguridad en iCloud);

→ ver notas, contactos, calendario, recordatorios, etc.;

→ y descargar todos los datos mediante herramientas de Apple.

Línea telefónica

Tener la línea telefónica comprometida es diferente a tener el celular o una cuenta invadida. Podemos considerar que una línea fue comprometida de dos formas principales: a través de una técnica llamada *SIM swap*, o mediante interceptación telefónica.

SIM swap

Ocurre cuando alguien logra **transferir tu número de teléfono a otro chip** sin tu autorización. Para ello, la

persona suele hacerse pasar por ti ante la operadora, usando tus datos personales, y solicita la sustitución del chip. Con acceso a tu línea, esa persona pasa a recibir tus mensajes SMS y llamadas, y puede, por ejemplo, recibir códigos para acceder a tu cuenta de WhatsApp, Signal o Telegram, por ejemplo. También podría irrumpir correos electrónicos y redes sociales mediante la opción de "olvidé mi contraseña".

Interceptación telefónica (pinchazo)

Sucede cuando alguien comienza a **interceptar el contenido de tus comunicaciones telefónicas**. Es decir, desde el momento en que tu número es intervenido, el contenido de tus llamadas realizadas mediante la red telefónica comienza a ser grabado. También se interceptan los SMS enviados y recibidos. Además, la información de geolocalización puede ser accedida en tiempo real. Cabe destacar que aquí nos referimos a comunicaciones realizadas por la red móvil, no por internet.

La interceptación telefónica puede hacerse **legalmente**, a través de un autorización judicial y en el marco de una investigación policial; o **ilegalmente**, utilizando

inesperadamente, se descargue la batería rápido o funcione raro.

Podría ocurrir:

- **Uso de funcionalidades de control parental** (como Family Link de Google) para localizarme, ver búsquedas en google maps, historial de ubicaciones, ver las búsquedas de google o bloquear el celular.

- **Uso de funcionalidades "buscar mi dispositivo"** para localizarme.

- **Uso de aplicaciones para espiar**, aunque se necesita haber accedido al celular por el tiempo suficiente para instalar y configurar la app.

- **Descargar apps fraudulentas o virus**, sin que eso implique que tu (ex)pareja tenga acceso o control de tu celular.

- **Sufrir estafas que guían la instalación de aplicaciones fraudulentas**, que puede implicar el acceso a tus datos por parte de les estafadores.

contraseña y pueda acceder desde otro dispositivo. Lo mismo para tu cuenta de Apple en iPhone.

- Si usas la misma contraseña para todas las cuentas y la compartiste alguna vez con tu (ex)pareja > lo más probable es que sepa la contraseña y pueda acceder desde otro dispositivo a tus redes sociales o cuenta de Google o Apple (si tienen esa misma contraseña).

- Si tu (ex)pareja tiene acceso a dispositivos (celular, laptop, tele, etc) dónde se quedó iniciada tu sesión de google > lo más probable es que tenga acceso a tu cuenta de google.

- Si tu teléfono está viejo, dañado o tiene pocos recursos > lo más probable es que funcione lento, se descargue la batería rápido o funcione raro.

- Si estás usando el celular más tiempo del habitual, debido a la situación de estrés > lo más probable es que la batería se descargue antes.

- Si tienes muchas aplicaciones instaladas y el almacenamiento interno está casi lleno > lo más probable es que funcione lento, las aplicaciones se cierren

equipos clandestinos o incluso mediante la corrupción de empleados. Este tipo de interceptación es un delito en muchos países y puede violar derechos constitucionales.

Entonces, **según sea el caso, el abordaje será distinto**, en esta tabla te hacemos un resumen:

¿Qué creo que fue intervenido?	**¿Qué podría hacer para detenerlo?**
Dispositivo (celular)	Analizar el dispositivo para detectar posible *malware*; revisar apps instaladas y permisos; revisar apps y funcionalidades de control parental; restaurar a valores de fábrica (se pierden todos los datos); sustituir dispositivo;
Cuenta vinculada (Google o Apple ID)	Cambiar contraseñas y métodos de recuperación de la cuenta; revisar sesiones iniciadas
Línea telefónica	Cambiar de número (de chip); evitar las llamadas por línea y SMS, hacer llamadas por WhatsApps o Signal (que no usan la línea telefónica sino internet); quitar teléfono intervenido de los métodos de recuperación de cuentas o autenticación de dos factores

*Muchas personas que sienten que fueron hackeadas tienen el impulso de **cambiar de número de teléfono (de chip)**, creyendo que eso implica un total cambio de vida digital, pero no es así. Un cambio de chip **no evita un acceso a la cuenta** de Google o de Apple ni **tampoco elimina un posible software espía** o aplicación de control parental. Esperamos que esta información te ayude a entender mejor y orientar tus futuras acciones.*

3. ¿Cómo funcionan los programas espía?

Cuando hablamos de un celular hackeado, es común pensar en la palabra *malware*. Este es un término genérico para referirse a programas maliciosos creados con el objetivo de causar daños, robar información o espiar dispositivos. Existen diferentes tipos de *malware*, como por ejemplo: virus, *worms*, trojanos, *adware*, *ransomware*, *RATs*, *spyware* (¡todas palabras en inglés!). La lista es extensa y, muchas veces, un sólo programa puede combinar varios tipos de *malware* en uno. Sin embargo, vale la pena prestar especial atención a los software espía que son utilizados con el objetivo de recolectar información sin el conocimiento ni consentimiento de la persona objetivo. Es decir, están diseñados para ser silenciosos, re-

Lo más probable / lo más común:

- **Acceso a cuentas de Google, Apple o redes sociales sin métodos muy técnicos**, porque se compartió la contraseña, se usa una contraseña sencilla de deducir, la misma para todos las cuentas, se compartieron dispositivos con las cuentas logueadas, se tienen hijes en común que pueden facilitar la contraseña o tienen celulares con tus cuentas loguedas. Es decir, acceso a cuentas aprovechando descuidos, uso de la tecnología sin muchas medidas de protección, brecha digital, etc.

- **Funcionamiento lento/raro del celular o descarga de batería**, porque es antiguo, tiene pocos recursos, hay muchas aplicaciones instaladas, se le da más uso en una situación de estrés.

- **Tener notificaciones de publicidad invasiva**, muy común en fabricantes de origen chino cómo Xiaomi.

Por ejemplo:

- Si tu (ex)pareja creó y configuró tu cuenta de Google en tu teléfono > lo más probable es que sepa la

cación en el proceso. Puedes comprobar enlaces sospechosos en *virustotal.com* o buscando en internet el mensaje que te llegó para saber más.

- **Malwarebytes te da una alerta** de haber encontrado algo sospechoso: Malwarebytes[9] es una aplicación confiable para revisar celulares. Puedes usar la versión de prueba para revisar tu dispositivo. Si te da una alerta de haber encontrado alguna aplicación potencialmente maliciosa, pide ayuda[10]. ¡Cuidado con otros antivirus para móviles, muchos traen publicidad muy invasiva y hasta puedan ser maliciosos!

7. ¿Qué pudo pasar?

Queremos mostrarte aquí un listado de posibles situaciones y cuánto de comunes/probables son, en base a nuestra experiencia trabajando con líneas de ayuda feminista. Una de las líneas de ayuda que entrevistamos llamaba a esta clasificación "pirámide de probabilidad".

¡Esperamos que te sirva para que hacerte a la idea de qué pudo pasar, pero todo depende tu caso y tu contexto!

9 https://www.malwarebytes.com/es/
10 Ver apartado 9.

copilando datos de la forma más imperceptible posible. Existen software espía más simples, como los usados en contextos de relaciones abusivas, y otros más sofisticados, como los utilizados por gobiernos y otros agentes maliciosos.

Software espía utilizado en relaciones afectivas (en ingles, *Spouseware* o *Stalkerware*)

Estos son software espía simples y accesibles. Generalmente se anuncian como herramientas de control parental y pueden adquirirse a bajo costo o incluso gratuitamente. Para instalarlos, alguien necesita tener acceso físico al celular objetivo y saber exactamente qué hacer, ya que rara vez están disponibles en tiendas como Play Store o App Store. Además de la instalación, a menudo es necesario realizar algunas configuraciones adicionales. Otra posibilidad es que se envíen a través de un enlace malicioso con la intención de engañar a la persona para que haga clic y descargue la app. En estos casos, el celular suele pedir permisos como acceso a la ubicación, cámara o mensajes. Es decir, aunque puedan ser sutiles, dejan señales claras de su instalación o configuración y no es difícil detectarlos.

Software espía sofisticado

Además del software espía utilizado en relaciones afectivas, también existe software espía altamente sofisticado, desarrollados por empresas especializadas en vigilancia digital y, en general, utilizados por gobiernos en contextos específicos. Estos programas suelen aprovechar vulnerabilidades aún desconocidas (vulnerabilidad de día cero[1]) y, en algunos casos, pueden acceder al dispositivo sin que la persona haga clic alguno. Un ejemplo es Pegasus[2], un software que ganó notoriedad por haber sido utilizado de forma abusiva para espiar a periodistas y activistas. Sin embargo, este tipo de tecnología tiene un costo muy elevado (de cientos de miles de dólares) y no se utiliza de forma masiva o indiscriminada. Son herramientas dirigidas, aplicadas en contextos muy específicos, y por eso no representan un riesgo real para el día a día de la mayoría de las personas. Son mucho más difíciles de detectar.

1 https://es.wikipedia.org/wiki/Ataque_de_d%C3%ADa_cero
2 https://es.wikipedia.org/wiki/Pegasus_(spyware)

cualquier buscador para saber qué es. Presta especial atención a las aplicaciones que tenga permisos de acceso al micrófono, cámara, geolocalización o accesibilidad. Pide ayuda[7] para la revisión de aplicaciones si tienes dudas.

- **Google Play Protect** está desactivado: esta es una funcionalidad de Google Play que impide la instalación de apps maliciosas, si está desactivado no es buena señal. Puedes comprobar su estado siguiendo esta documentación de Google[8].

- **La opción "Instalar Apps desconocidas" está activada** para algún navegador o el gestor de archivos: esta opción permite la instalación de apps sin hacer uso de Google Play. Estas apps no pasan por la verificación de Google Play y pueden ser maliciosas.

- **Hiciste clic en algún** enlace sin fijarte mucho: si te llegó un mensaje que entendiste como confiable e hiciste clic en el enlace que te indicaba, mantén la calma, a todes nos puede pasar. Sin embargo, si podría ser preocupante si se descargó o instaló alguna apli-

7 Ver apartado 9.
8 https://support.google.com/android/answer/2812853?hl=es

sistema de internet y se hace masivamente. Mediante una solicitud de seguimiento NO es posible intervenir una cuenta ni un celular.

- "**Personas desconocidas me hablaron** en WhatsApp o en redes sociales": hay intentos masivos de establecer conversaciones por estos medios. Suelen ser estafas o simplemente formas de comprobar que un número existe. Puedes reportar y bloquear o simplemente no contestar.

Estos son algunos indicadores a los que **sí deberías prestar atención**:

- **Encuentras aplicaciones nuevas que no reconoces**: pero tranqui, no paniquees demasiado rápido, hay muchas aplicaciones del sistema que quizás no reconoces pero que es normal que estén ahí y son necesarias para que el celular funcione. Si dudas puedes buscar en internet el nombre de la aplicación que te parece sospechosa. Estas son dos webs de referencia que te pueden ayudar a saber más sobre una aplicación: *immuniweb.com* y *reports.exodus-privacy.eu.org*. También puedes buscar el nombre de la aplicación en

Registrador de teclado (en inglés, *keylogger*)

Son programas maliciosos diseñados para capturar y registrar cada tecla presionada en el teclado de un dispositivo, monitoreando todo lo que se escribe. Pueden ser usados para robar contraseñas, datos bancarios, monitorear comunicaciones privadas, etc. En celulares, pueden estar presentes en aplicaciones de teclado alternativas, herramientas de control parental o software espía utilizado en relaciones afectivas, o incluso en aplicaciones que abusan de los servicios de accesibilidad para leer texto en campos sensibles.

4. ¿Aplicaciones para proteger o para controlar?

Aplicaciones creadas para el control parental, como Google Family Link, Life360 o aplicaciones de rastreo, han sido cada vez más **utilizadas en relaciones afectivas como herramientas de control y vigilancia**. Vendidas bajo el discurso de la seguridad y la protección familiar, muchas terminan siendo usadas por parejas para monitorear la ubicación, el historial de llamadas, redes sociales e incluso el tiempo de pantalla, sin consentimiento.

Además de las aplicaciones más conocidas, también existe un mercado silencioso de software espía utilizado en relaciones afectivas que se disfraza como herramientas de control parental pero que claramente fueron diseñadas para ser utilizadas en el contexto de relaciones afectivas. Muchas de estas pueden encontrarse fácilmente en la web, no en tiendas oficiales de aplicaciones, sino en sitios propios de apariencia profesional que ofrecen "monitoreo familiar", "rastreo de empleados" o "protección de seres queridos".

La línea entre protección y control es muy delgada. En cualquier relación, ya sea con hijes o con parejas, es natural querer proteger a quienes se ama. Pero existe una diferencia fundamental. Cuando el cuidado se convierte en vigilancia sin consentimiento, cuando la protección se basa en la desconfianza, lo que parecía protección puede rápidamente transformarse en control y violencia.

5. Seguramente no es hacker

Compañera, compañere, creemos que es importante que tengas esta información. Quizás tu pareja o expareja

- "**Tengo notificaciones raras**": algunos celulares de fabricantes chinos (cómo Xiaomi) traen mucha publicidad en sus aplicaciones. Esta publicidad a veces es muy invasiva y aparece en forma de notificación. Revisa la configuración de tus aplicaciones y sus notificaciones. Si sigues con notificaciones que no vinculas a ninguna aplicación y no consigues desactivarlas entonces sí deberías pedir ayuda[5].

- "**Veo alertas de virus**" en el navegador: lo más probable es que estés visitando una webs que está mostrando una alerta falsa de virus para que te asustes y hagas clic en ellas. Su intención suele ser maliciosa. No hagas clic en ninguna alerta, presta atención, a veces parecen muy reales y es fácil confundirse. Este es un fenómeno tristemente habitual en internet[6].

- "**Me llegaron solicitudes de seguimiento en redes sociales**": nos llegan cientos de solicitudes se seguimiento en redes sociales, es algo habitual en el eco-

5 Ver apartado 9
6 https://www.incibe.es/ciudadania/blog/que-significan-los-mensajes-y-notificaciones-que-aparecen-al-navegar-por-internet

6. Qué síntomas son preocupantes y cuáles no

En una situación de estrés y angustia **es muy habitual estar alerta y prestar mucha atención al comportamiento de nuestros dispositivos**. De forma similar a cuando enfrentamos algún problema de salud, que nos fijamos más en el comportamiento de nuestro cuerpo y de pronto identificamos nuevos síntomas que no sabemos si ya estaban antes, desde cuando o si guardan relación.

Estos son algunos síntomas que puedes empezar a observar pero que por sí solos **NO son preocupantes**:

- "**Siento que la batería de mi celular se descarga muy rápido**": probablemente tú celular ya tiene más de dos años, tienes bastantes apps instaladas, estos días de estrés te comunicas más con tus seres queridos y haces un mayor uso de redes sociales; todo ello hace que la batería se descargue más rápido.

- "**Mi celular funciona lento**": si tiene muchas apps abiertas, ya tiene unos años y no es un modelo muy potente... es bastante normal que un celu vaya lento.

dijo que era hacker o que conocía hackers, quizás te hizo creer que sabe mucho de tecnología y es capaz de "hackear" dispositivos "por arte de magia". La realidad es que no es así.

La idea de "hacker" que tenemos en la cabeza es sólo una ficción de las películas. Sin embargo, funciona en nuestros imaginarios y nos hace pensar que alguien con unos conocimientos extraordinarios puede vulnerar los sistemas de protección de nuestros dispositivos. La verdad es que para que un dispositivo o una aplicación salga al mercado tienen que pasar por muchos controles de seguridad antes de llegar a tus manos. Hay equipos de personas que se dedican a hacer este trabajo todos los días. Cuando se detecta una vulnerabilidad de seguridad se lanzan inmediatamente actualizaciones para paliar las vulnerabilidades.

Por mucho que tu pareja o expareja haya estudiado informática, dedique muchas horas en la computadora o diga que es una persona "experta" en la materia, recuerda que:

→ **No puede acceder a tu dispositivo de forma remota** "por arte de magia". Para eso tendría que haber accedido físicamente al celular y haber instalado alguna aplicación para ello. Piensa si pudo tener acceso físico al celular, con suficiente tiempo para instalar una app. Si es así, puedes hacer una revisión de tus apps instaladas o pedir ayuda para la revisión de tu celular[3].

→ **No puede acceder a tus cuentas** si no tiene manera de saber la contraseña y la cuenta no se quedó iniciada en algún dispositivo que puedas haber compartido con esta persona. Si tienes dudas: fortalece tus contraseñas y revisas las sesiones iniciadas. Si lo necesitas, puedes pedir ayuda a una línea de atención feminista para que te acompañe en este proceso[4].

Además, queremos contarte que la mayoría de veces que alguien dice que es "hacker", lo que hace es usar:

• **Métodos de ingeniería social**, es decir, diferentes formas de influir, manipular o engañar para que la persona comparta contraseñas o códigos de seguridad. Puede utilizar a familiares, amigues o hijes que se tienen en común para acceder a esta información.

3 Ver apartados 9 y 10.
4 Idem

• **Fuentes abiertas** y datos que hay publicados en internet para obtener información personal de la persona e incluso simular que ha accedido a dispositivos cuando en realidad solo ha buscado esos datos en internet.

¡Cuidado con los correos de recuperación de las cuentas! *No hace falta saber mucho para hacer clic en "olvidé la contraseña" en Instagram, Facebook o cualquier otra red social y que se envíe al correo de recuperación el enlace que permite el cambio de contraseña. Si este correo de recuperación es antiguo, no lo revisas a menudo, tiene la contraseña que usas para todo y lo compartiste con tu (ex)pareja... pues fácilmente puede acceder y cambiar la contraseña de tu cuenta. Esta es una forma muy habitual de acceso no deseado y secuestro de cuentas por parte de familiares o (ex)parejas. Recuerda poner tu correo electrónico actualizado y protegido con una buena contraseña.*