El estado del **stalkerware** en 2022

Coalition Against Stalkerware

kaspersky

Índice

Hallazgos principales en 2022

El estado del stalkerware es un informe anual de Kaspersky que contribuye a comprender mejor cuánta gente en el mundo se ve afectada por el acoso digital. El stalkerware es un software disponible en el mercado que se puede instalar discretamente en dispositivos de teléfonos inteligentes y permite a los agresores monitorear la vida privada de una persona sin su conocimiento.

Cualquier persona con una conexión a Internet y acceso físico a un teléfono inteligente puede descargar e instalar stalkerware fácilmente. El agresor viola la privacidad de la víctima, ya que puede utilizar el software para monitorear enormes volúmenes de datos personales. Dependiendo del tipo de software, normalmente es posible comprobar la ubicación del dispositivo, los mensajes de texto, los chats en las redes sociales, las fotos, el historial del navegador y más. El stalkerware funciona en segundo plano, lo que significa que la mayoría de las víctimas no saben que cada uno de sus pasos y acciones está siendo monitoreado.

En la mayoría de los países del mundo, el uso del software stalkerware actualmente no está prohibido, pero instalar una aplicación de este tipo en el teléfono inteligente de otra persona sin su consentimiento es ilegal y está penado. Sin embargo, el responsable será el infractor, no el desarrollador de la aplicación.

Junto con otras tecnologías relacionadas, el stalkerware forma parte del abuso impulsado por la tecnología y, a menudo, se usa en relaciones abusivas. Como esto forma parte de un problema más amplio, Kaspersky trabaja con expertos y organizaciones relevantes en el campo de la violencia doméstica, desde servicios de apoyo a las víctimas y programas para agresores hasta agencias gubernamentales y de investigación, para compartir conocimientos y apoyar tanto a los profesionales como a las víctimas.

Datos destacados de 2022

- **En 2022, los datos de Kaspersky muestran que 29 312 personas únicas en todo el mundo se vieron afectadas por el stalkerware.** En comparación con la tendencia a la baja que se había registrado en años anteriores, es similar al número total de usuarios afectados en 2021. Teniendo en cuenta los avances en el software de acoso digital en los últimos años, los datos sugieren que hay una tendencia hacia la estabilización. En términos más generales, es importante señalar que los datos cubren el número de usuarios afectados de Kaspersky, y es probable que el número global de personas afectadas sea mucho mayor. Algunos usuarios afectados podrían utilizar otra solución de ciberseguridad en sus dispositivos, mientras que otros no utilizan ninguna solución en absoluto.
- **Además, los datos revelan una proliferación estable del stalkerware durante los 12 meses de 2022.** En promedio, cada mes, 3,333 usuarios se vieron afectados por el stalkerware por primera vez. La tasa de detección estable indica que el acoso digital se ha convertido en un problema persistente que merece una mayor atención por parte de la sociedad. Los miembros de la Coalición contra el stalkerware estima que podría haber cerca de un millón de víctimas en todo el mundo afectadas por el stalkerware cada año.
- Según Kaspersky Security Network, **el stalkerware se usa con mayor frecuencia en Rusia, Brasil e India,** pero sigue siendo un fenómeno mundial que afecta a todos los países. A nivel regional, los datos revelan que el mayor número de usuarios afectados se encuentra en los siguientes países:
  - Alemania, Italia y Francia (Europa);
  - Irán, Turquía y Arabia Saudí (Oriente Medio y África);
  - India, Indonesia y Australia (Asia-Pacífico);
  - Brasil, México y Ecuador (América Latina);
  - Estados Unidos (Norteamérica);
  - Federación de Rusia, Kazajstán y Bielorrusia (Europa del Este [excepto los países de la Unión Europea], Rusia y Asia Central).
- A escala mundial, la aplicación de stalkerware más utilizada es Reptilicus, con 4.065 usuarios afectados.

Tendencias de 2022 observadas por Kaspersky

En 2022, un total de 29 312 usuarios individuales se vieron afectados por el stalkerware

Cifras de detección mundial: usuarios afectados

En esta sección se comparan las estadísticas globales y regionales recopiladas por Kaspersky en 2022 con las estadísticas de años anteriores. En 2022, el stalkerware afectó a un total de 29 312 usuarios únicos. El gráfico 1 a continuación muestra cómo este número ha variado de un año a otro desde 2018.

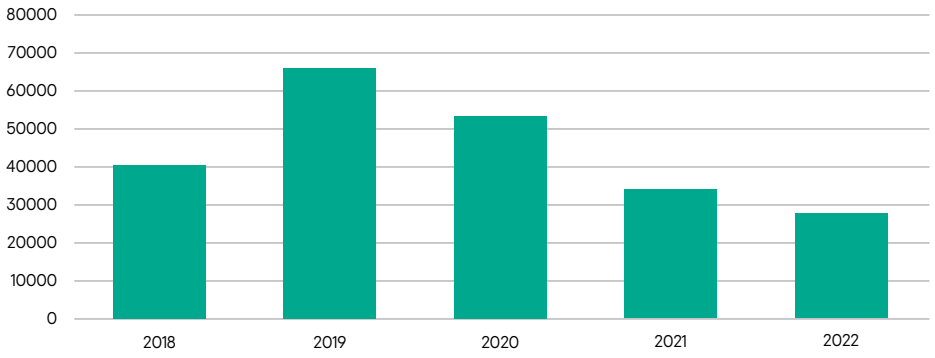


Gráfico 1: Evolución interanual de los usuarios afectados desde 2018

El gráfico 2 a continuación muestra el número de usuarios únicos afectados por mes entre 2021 y 2022. En 2022, la situación es casi idéntica a la de 2021, lo que indica que el ritmo de proliferación del stalkerware se ha estabilizado. De media, 3333 usuarios se vieron afectados por el stalkerware por primera vez cada mes.

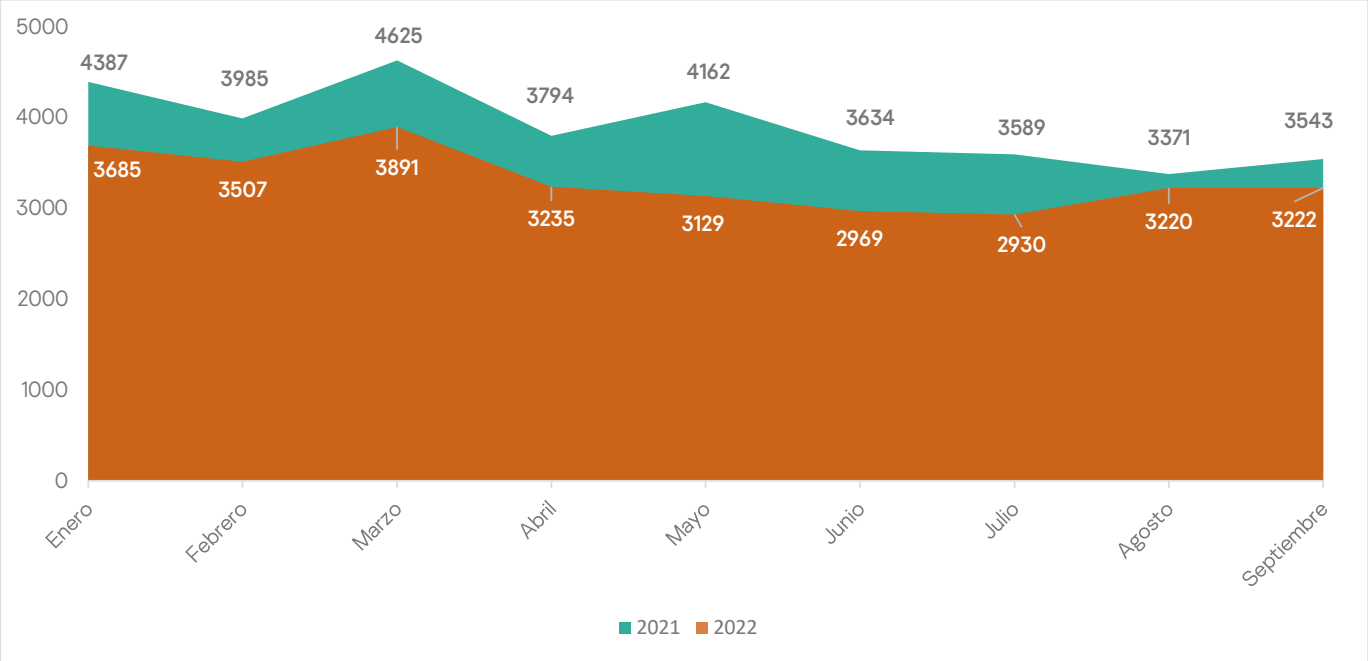
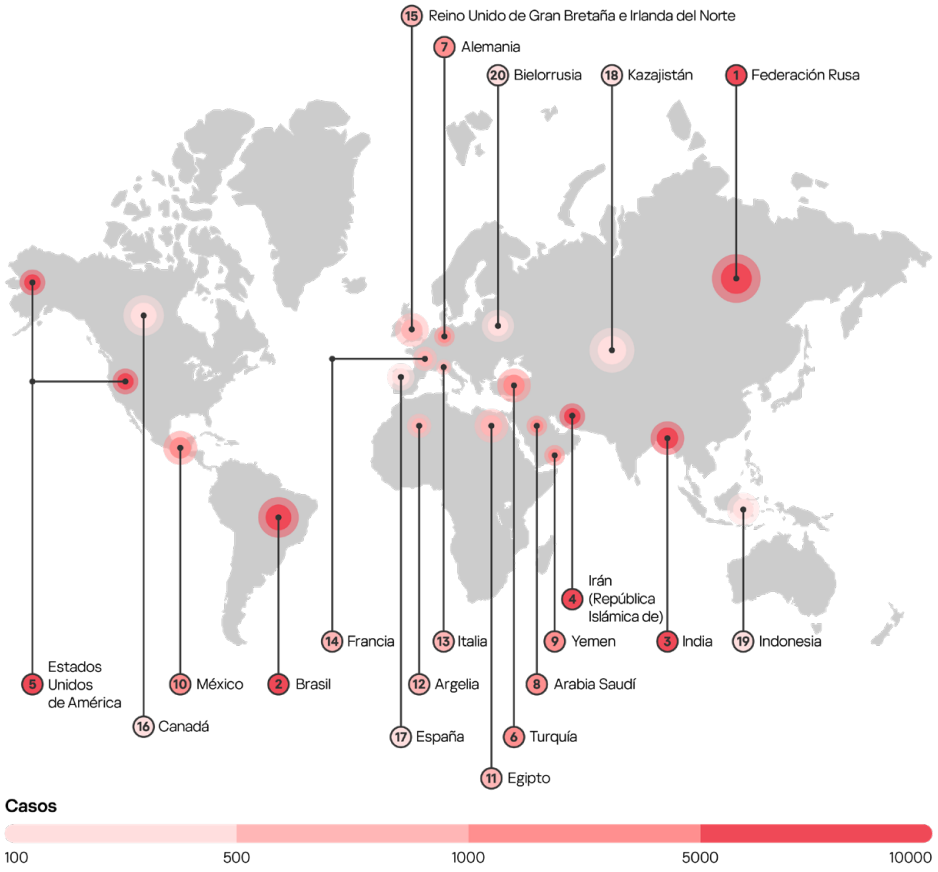


Gráfico 2: Usuarios afectados únicos mensuales de 2021 a 2022

Cifras de detección mundial y regional: geografía de los usuarios afectados

El stalkerware sigue siendo un problema mundial. En 2022, Kaspersky detectó usuarios afectados en 176 países.



Mapa 1: Países más afectados por el stalkerware en 2022

Metodología

Los datos de este informe se han extraído de las estadísticas agregadas de amenazas obtenidas de Kaspersky Security Network. Kaspersky Security Network se dedica a procesar los flujos de datos relacionados con la ciberseguridad de millones de participantes voluntarios de todo el mundo. Todos los datos recibidos se anonimizan. Para calcular las estadísticas, se ha revisado la gama de soluciones de seguridad móvil de Kaspersky para consumidores de acuerdo con los criterios de detección de stalkerware de la Coalición contra el Stalkerware. Esto significa que el número de usuarios afectados ha sido atacado únicamente por stalkerware. Otros tipos de aplicaciones de monitoreo o software espía que no entran en la definición de la Coalición no se incluyen en las estadísticas del informe.

Las estadísticas reflejan los usuarios móviles únicos afectados por el stalkerware, que es diferente del número total de detecciones. El número de detecciones puede ser mayor, ya que es posible que se haya detectado stalkerware varias veces en el mismo dispositivo del mismo usuario único si este ha decidido no eliminar la aplicación al recibir una notificación.

Por último, las estadísticas solo reflejan a los usuarios móviles que utilizan las soluciones de seguridad de TI de Kaspersky. Algunos usuarios pueden utilizar otra solución de ciberseguridad en sus dispositivos, mientras que otros no utilizan ninguna solución en absoluto.

En 2022, Rusia (8,281), Brasil (4,969) e India (1,807) fueron los tres países con más usuarios afectados. Esos tres países se mantienen en las primeras posiciones según las estadísticas de Kaspersky desde 2019. En comparación con años anteriores, cabe destacar que el número de usuarios afectados en EE. UU. ha bajado en la clasificación y ahora ocupa el quinto lugar con 1,295 usuarios afectados. Por el contrario, se ha observado un aumento en Irán, que ha subido al cuarto lugar con 1754 usuarios afectados.

Sin embargo, en comparación con 2021, solo Irán figura como nuevo participante entre los 5 países más afectados. Los otros cuatro países (Rusia, Brasil, India y EE. UU.) han figurado tradicionalmente en la parte superior de la lista. Si observamos la otra mitad de los 10 países más afectados, Turquía, Alemania y México se han mantenido entre los países con más afectados en comparación con el año pasado. Entre los 10 países más afectados en 2022 se encuentran Arabia Saudí y Yemen.

	País	Usuarios afectados
1	Federación Rusa	8,281
2	Brasil	4,969
3	India	1,807
4	Irán	1,754
5	Estados Unidos de América	1,295
6	Turquía	755
7	Alemania	736
8	Arabia Saudí	612
9	Yemen	527
10	México	474

Tabla 1: Los 10 países más afectados por el stalkerware en el mundo en 2022

En Europa, el número total de usuarios únicos afectados en 2022 ascendió a 3,158. Los tres países más afectados de Europa fueron Alemania (737), Italia (405) y Francia (365). En comparación con 2021, todos los países hasta el séptimo lugar de la lista (los Países Bajos) siguen figurando como los países más afectados de Europa. Los nuevos participantes en la lista son Suiza, Austria y Grecia.

	País	Usuarios afectados
1	Alemania	736
2	Italia	405
3	Francia	365
4	Reino Unido	313
5	España	296
6	Polonia	220
7	Países Bajos	154
8	Suiza	123
9	Austria	71
10	Grecia	70

Tabla 2: Los 10 países más afectados por el stalkerware en Europa en 2022

En Europa del Este (excluidos los países de la Unión Europea), Rusia y Asia Central, el número total de usuarios únicos afectados en 2022 ascendió a 9,406. Los tres primeros países fueron Rusia, Kazajistán y Bielorrusia.

	País	Usuarios afectados
1	Federación Rusa	8,281
2	Kazajistán	296
3	Bielorrusia	267
4	Ucrania	258
5	Azerbaiyán	130
6	Uzbekistán	76
7	Moldavia	34
8	Tayikistán	32
9	Kirguistán	31
10	Armenia	27

Tabla 3: Los 10 países más afectados por el acoso en Europa del Este (excluidos los países de la UE), Rusia y Asia Central en 2022

En la región de Oriente Medio y África, el número total de usuarios afectados fue de 6,330, una cifra ligeramente superior a la de 2021. Mientras tanto, Irán, con 1,754 usuarios afectados, encabeza la lista en 2022, mientras que los 755 usuarios afectados de Turquía han llevado al país al segundo lugar de la región, seguido de cerca por Arabia Saudí, con 612 usuarios afectados.

	País	Usuarios afectados
1	Irán	1,754
2	Turquía	755
3	Arabia Saudí	612
4	Yemen	527
5	Egipto	469
6	Argelia	407
7	Marruecos	168
8	Emiratos Árabes Unidos	155
9	Sudáfrica	145
10	Kenia	123

Tabla 4: Los 10 países más afectados por el stalkerware en Oriente Medio y África en 2022

En la región de Asia-Pacífico, el número total de usuarios afectados fue de 3187. La India sigue muy por delante de los demás países de la región, con 1807 usuarios afectados. Indonesia ocupa el segundo lugar con 269 usuarios afectados, mientras que Australia ocupa el tercer lugar con 190 usuarios afectados.

	País	Usuarios afectados
1	India	1,807
2	Indonesia	269
3	Australia	190
4	Filipinas	134
5	Malasia	129
6	Vietnam	109
7	Bangladés	105
8	Japón	95
9	Tailandia	52
10	Pakistán	48

Tabla 5: Los 10 países más afectados por el stalkerware en la región de Asia-Pacífico en 2022

La región de América Latina y el Caribe está dominada por Brasil, con 4,969 usuarios afectados. Esto representa aproximadamente el 32 % del número total de usuarios afectados de la región. A Brasil le siguen México y Ecuador en la lista, mientras que Colombia ha pasado al cuarto lugar. Se ha registrado un número total de 6,170 usuarios afectados en la región.

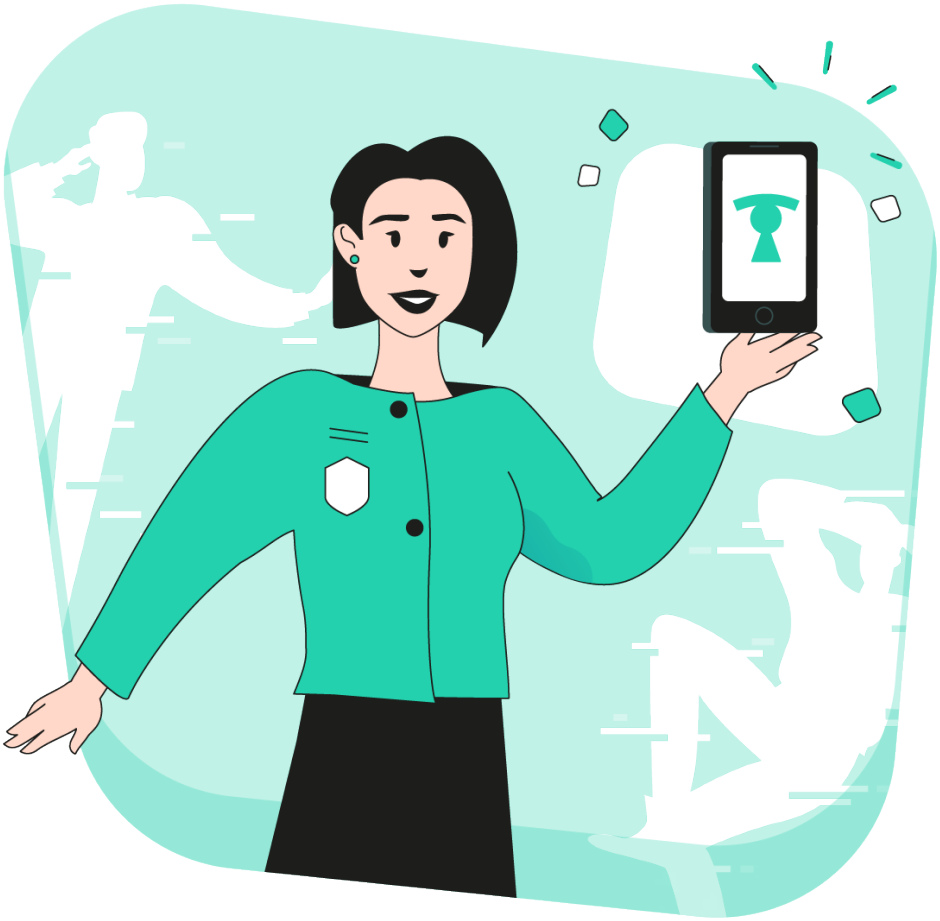
	País	Usuarios afectados
1	Brasil	4,969
2	México	474
3	Ecuador	146
4	Colombia	120
5	Perú	111
6	Argentina	85
7	Chile	49
8	Bolivia	32
9	Venezuela	30
10	República Dominicana	24

Tabla 6: Los 10 países más afectados por el stalkerware en América Latina en 2022

Por último, en Norteamérica, el 87 % de todos los usuarios afectados de la región se encuentran en los Estados Unidos. Esto es de esperar, dado el tamaño relativo de la población de los Estados Unidos en comparación con Canadá. En toda la región de Norteamérica se vieron afectados un total de 1,585 usuarios.

	País	Usuarios afectados
1	Estados Unidos de América	1,295
2	Canadá	299

Tabla 7: Cantidad de usuarios afectados por el stalkerware en Norteamérica en 2022



Cifras de detección mundial: aplicaciones de stalkerware

En este apartado se enumeran las aplicaciones de stalkerware más utilizadas para controlar teléfonos inteligentes en todo el mundo. En 2022, la aplicación más popular fue Reptilicus (4,065 usuarios afectados). Este año Kaspersky ha detectado 182 aplicaciones diferentes de stalkerware.

	Nombre de aplicación	Usuarios afectados
1	Reptilicus (también conocida como Vkurse)	4,065
2	Cerbero	2,407
3	KeyLog	1,721
4	MobileTracker	1,633
5	wSpy	1,342
6	SpyPhone	1,211
7	Anlost	1,189
8	Track My Phones	1,137
9	MonitorMinor	864
10	Hovermon	827

Tabla 8: Las 10 aplicaciones de stalkerware principales en 2022

El stalkerware proporciona un medio para controlar la vida de una víctima. Sus capacidades varían según el tipo de aplicación y si se ha pagado o se ha obtenido de forma gratuita. Por lo general, el stalkerware se hace pasar por aplicaciones antirrobo o de control parental legítimas, cuando en realidad son muy diferentes, sobre todo debido a que se instalan sin el consentimiento ni notificación de la persona que está siendo rastreada, y a que funcionan de forma sigilosa en los dispositivos de teléfonos inteligentes.

¿El stalkerware afecta por igual a dispositivos con SO Android e iOS?

Las herramientas de stalkerware son menos frecuentes en los iPhones que en los dispositivos Android porque iOS es tradicionalmente un sistema cerrado. Sin embargo, los delincuentes pueden evitar esta limitación en los iPhones con «jailbreak», aunque siguen necesitando acceso físico directo al teléfono para hacerlo. Los usuarios de iPhone que teman ser vigilados siempre deben vigilar su dispositivo.

Alternativamente, un infractor puede ofrecer a su víctima un iPhone, o cualquier otro dispositivo, con un stalkerware preinstalado. Hay muchas empresas que ofrecen estos servicios en línea, lo que permite a los abusadores instalar estas herramientas en los teléfonos nuevos, que luego se pueden entregar en el embalaje de fábrica con el pretexto de obsequiar a la víctima prevista.

A continuación se muestran algunas de las funciones más comunes que pueden estar presentes en las aplicaciones de stalkerware:

- Ocultar el icono de la aplicación
- Lectura de SMS, MMS y registros de llamada
- Obtención de listas de contactos
- Rastreo de la ubicación por GPS
- Rastreo de eventos de calendario
- Lectura de mensajes de servicios de mensajería y redes sociales populares, como Facebook, WhatsApp, Signal, Telegram, Viber, Instagram, Skype, Hangouts, Line, Kik, WeChat, Tinder, IMO, Gmail, Tango, SnapChat, Hike, TikTok, Kwai, Badoo, BBM, TextMe, Tumblr, Weico, Reddit, etc.
- Visionado de fotos e imágenes de las galerías de imágenes de los teléfonos
- Capturas de pantalla
- Hacer fotos con la cámara frontal (modo autofoto)

Acoso digital y violencia de género

El stalkerware es un método de ciberacoso que forma parte de la violencia digital

Tanto las mujeres como los hombres pueden ser víctimas de la violencia digital, pero las investigaciones muestran que, en la inmensa mayoría de los casos, las mujeres son el objetivo debido a su género. Es importante recordar que la violencia digital es otra dimensión de la violencia. Debe entenderse como un continuo de violencia física, ya que tiene efectos reales y negativos en las víctimas. Para obtener más información, lea la hoja informativa "Ciberviolencia contra mujeres y niñas: Términos y conceptos clave" (2022) publicado por el Instituto Europeo de Igualdad de Género.

La importancia de los datos para comprender el alcance de la violencia digital — Dra. Leonie Maria Tanczer, profesora asociada del University College de Londres y responsable del Grupo de Investigación sobre Género y Tecnología de la UCL

Las investigaciones anteriores sobre las formas de acoso y violencia de género facilitadas por la tecnología se han centrado en una serie de sistemas digitales "cotidianos" que pueden funcionar como herramientas para coaccionar, controlar y dañar a una persona o a grupos de personas. Aunque el informe y los datos actuales se limitan a los dispositivos móviles, el acoso digital puede facilitarse a través de otros, incluidos los rastreadores GPS o el llamado "Internet de las cosas" (IoT). Este último incluye productos inteligentes con conexión a Internet, como timbres de casa inteligentes, cámaras de circuito cerrado de televisión o altavoces.

Las pruebas basadas en el abuso por medio de la tecnología también son aún muy limitadas. Los centros de investigación actuales se ubican en Australia, Reino Unido y Estados Unidos. En consecuencia, la mayoría de los estudios se centran en datos procedentes de estos países, lo que crea puntos ciegos. Los datos proporcionados en este informe contribuyen a una comprensión más amplia del panorama del abuso facilitado por la tecnología, que se necesita con urgencia.

También se ha demostrado que los servicios de apoyo a las víctimas se enfrentan a las crecientes demandas para mantenerse actualizado ante los avances tecnológicos. Han solicitado complementos a las actuales prácticas de evaluación de riesgos y seguridad, incluidos "planes de acción contra el ciberacoso" y formación específica para aumentar las aptitudes y la capacidad de respuesta del sector. De hecho, cada vez hay más ofertas de servicios especializados, como demuestran el equipo Tech Safety de Refuge, el proyecto Safety Net de la Red Nacional para Acabar con la Violencia Doméstica (NNEDV) o la Clínica para Acabar con el Abuso Tecnológico (CETA).

El Grupo de Investigación sobre Género y Tecnología del University College de Londres (UCL) investiga los puntos de intersección entre tecnología, seguridad y género para conseguir que los sistemas digitales funcionen para todos. Más información:

https://www.ucl.ac.uk/computer-science/research/research-groups/gender-and-tech

Prestar más atención a quienes sufren violencia digital — Elena Gajotto, vicepresidenta de Una Casa Per L'Uomo

El ciberacoso tiene un impacto concreto en la vida real de quienes lo sufren. Hay efectos psicológicos, físicos y sociales a mediano y largo plazo que vemos a diario en nuestros centros antiviolencia. Como subraya el Servicio de Investigación del Parlamento Europeo en su estudio (2021), todas las mujeres pueden ser víctimas potenciales del ciberacoso, ya sean personajes públicos, exparejas o simples usuarias de las redes sociales. El ciberacoso engloba diferentes tipos de comportamientos, como la mensajería persistente, el seguimiento de la actividad de la víctima u otras formas de persecución en línea, y como afirma el mismo estudio, "puede que el ciberacoso sea simplemente una pieza más en la caja de herramientas del acosador".

Cuando se trabaja con temas de violencia digital, hay que tener en cuenta las siguientes características:

- La violencia digital puede ejercerse junto con otras formas de agresión, ya sea física, sexual, psicológica, económica, etc.
- La violencia puede comenzar en línea y continuar fuera de ella o, viceversa, puede comenzar en el mundo fuera de línea y continuar en la esfera digital.
- No es sencillo eliminar -de forma permanente- los contenidos ofensivos, violentos o provocadores publicados en línea.
- Los actores de la violencia digital pueden ser individuos o grupos, y pueden ser tanto conocidos como desconocidos para la víctima.
- La violencia digital puede ejercerse a través de una amplia gama de dispositivos (computadoras, smartphones, dispositivos domésticos inteligentes, etc.) y en muchas plataformas diferentes (sitios web, aplicaciones de mensajería instantánea, chats en línea, redes sociales, etc.).

Como se ha mencionado, a pesar de ejercerse en el mundo digital, estas formas de violencia tienen un impacto profundo y tangible en la vida real de las víctimas. Los estudios demuestran que las mujeres son las principales víctimas del ciberacoso o de otras formas de violencia digital. Experimentan muchos de los mismos síntomas que las víctimas de la violencia offline, como, por ejemplo: ansiedad, ataques de pánico, trastorno de estrés postraumático (TEPT), pensamientos suicidas, ira, falta de confianza en sí mismas y dificultades de concentración. También puede haber efectos negativos económicos (extorsión, pérdida de ingresos, etc.) y sociales (pérdida de la red familiar y de amigos, aislamiento, etc.). Además, la violencia digital también tiene un impacto colectivo,

Una Casa Per L'Uomo es una organización de la sociedad civil italiana que gestiona servicios de apoyo a las víctimas. Ha sido socia del consorcio del proyecto DeStalk (2021-2023), cofinanciado por el Programa de Derechos, Igualdad y Ciudadanía de la Unión Europea, y es miembro de la Coalición contra el Stalkerware.

tanto a nivel económico como político, con un aumento de los costos públicos legales, administrativos y sanitarios, por un lado, así como una menor participación en el discurso público por parte de las mujeres.

Por eso es importante insistir en el peligro de este fenómeno. La sociedad debe prestar más atención al sufrimiento de la violencia digital. Con este objetivo, estamos trabajando con nuestros miembros, así como con Kaspersky y todos los socios de la Coalición contra el Stalkerware para apoyar a las víctimas y formar mejor a los profesionales que trabajan en el ámbito de la violencia doméstica.

Abordar las actitudes sociales que favorecen los abusos facilitados por la tecnología — Anna McKenzie, directora de Comunicación de WWP EN

Los abusos facilitados por la tecnología, como el stalkerware, preocupan cada vez más a nuestras organizaciones socias que trabajan en el cambio de comportamiento con agresores de violencia doméstica.

La violencia digital sigue aumentando: los dispositivos digitales, el software de vigilancia secreta y los espacios en línea ofrecen el entorno perfecto para que los individuos abusivos amplíen el control sobre la vida de sus parejas. Sin embargo, revisar el teléfono de la pareja, leer su correo electrónico, estar al tanto de su ubicación y conocer sus contraseñas es ahora algo tan habitual que a menudo las personas ni siquiera se dan cuenta de que están mostrando comportamientos abusivos.

¿Cómo es posible que estas aparentes violaciones de la intimidad no se perciban como tales?

En 2021, Kaspersky publicó el "Informe sobre el acoso digital en las relaciones", destacando algunas tendencias preocupantes. Según los datos, comportamientos como el seguimiento de las actividades digitales de la pareja con su consentimiento se consideraban en gran medida aceptables para garantizar la transparencia en una relación. Sin embargo, resulta preocupante que casi un tercio de los encuestados se muestren de acuerdo con vigilar las actividades de su pareja sin su consentimiento, especialmente si creen que su pareja les está siendo infiel.

Estas actitudes hablan directamente de los problemas que nuestros miembros encuentran regularmente en su trabajo con los actores de la violencia doméstica. Es muy problemático suponer que el hecho de que una persona no consienta el control significa que está ocultando una posible infidelidad. En las relaciones abusivas, el consentimiento es mínimo en el mejor de los casos: ¿Cómo pueden decir que sí, si después de todo, no pueden decir que no? Asimismo, la aceptación de la sospecha de infidelidad como excusa para espiar a la pareja es una oportunidad de oro para las parejas acosadoras, que perciben constantemente una amenaza de engaño en sus relaciones. Esto también habla de un sentido de propiedad y de una falta de comunicación sana, que son preocupaciones centrales en las relaciones abusivas.

Creemos que, más allá de la obvia necesidad de regulación legal, capacitación y concienciación general sobre el tema de la violencia digital, es de suma importancia que las actitudes de apoyo al abuso facilitado por la tecnología se aborden de forma generalizada y desde una edad temprana. Estudios como el informe State of Stalkerware son un importante control del statu quo, pero debemos hacer más para cambiarlo. Con la campaña #NoExcuse4Abuse, desarrollada y aplicada en colaboración con Kaspersky, hemos dado un primer paso para hacer frente a las actitudes sociales nocivas hacia el abuso facilitado por la tecnología y el stalkerware.

WWP EN es una red europea con 69 miembros de 34 países. Creemos que sin un enfoque que se dirija a los autores de la violencia doméstica y les exija responsabilidades, cualquier estrategia para acabar con la violencia de pareja está incompleta. Nuestro trabajo se centra en poner fin a la violencia de los hombres, exigirles responsabilidades y promover el Convenio de Estambul. Más información:

https://www.work-with-perpetrators.eu

Juntos seguimos luchando contra el stalkerware

Ante todo, el stalkerware no es un problema técnico, sino la expresión de un problema dentro de la sociedad que, por lo tanto, requiere la acción de todos los ámbitos de la sociedad. Kaspersky no solo se compromete activamente a proteger a los usuarios contra esta amenaza, sino que también mantiene un diálogo a varios niveles con organizaciones sin ánimo de lucro y agencias industriales, públicas y de investigación de todo el mundo para trabajar juntos en soluciones que aborden el problema.

En 2019, Kaspersky fue la primera empresa de ciberseguridad del sector en desarrollar una nueva alerta que notifica claramente a los usuarios si se encuentra stalkerware en sus dispositivos. Si bien las soluciones de Kaspersky llevan muchos años detectando

las aplicaciones potencialmente dañinas que no son malware (incluido el stalkerware), la nueva notificación alerta al usuario de que se ha encontrado una aplicación en su dispositivo que podría espiarlo.

En 2022, como parte del lanzamiento por parte de Kaspersky de una nueva cartera de productos de consumo, se amplió la alerta de privacidad y ahora no solo informa al usuario sobre la presencia de stalkerware en el dispositivo, sino que también le advierte de que, si se elimina el stalkerware, se avisará a la persona que ha instalado la aplicación. Esto puede llevar a un agravamiento de la situación. Además, el usuario corre el riesgo de borrar datos o pruebas importantes que podrían utilizarse en un proceso judicial.

En 2019, Kaspersky también cofundó Coalición Contra el Stalkerware, un grupo de trabajo internacional contra el stalkerware y la violencia doméstica que reúne a empresas privadas de TI, ONG, instituciones de investigación y organismos policiales que trabajan para combatir el ciberacoso y ayudar a las víctimas de abuso en Internet. A través de un consorcio de más de 40 organizaciones, las partes interesadas pueden compartir experiencias y trabajar juntas para resolver el problema de la violencia en Internet. Además, el sitio web de la Coalición, que está disponible en 7 idiomas diferentes, ofrece a las víctimas ayuda y orientación en caso de que sospechen que hay stalkerware en sus dispositivos.

De 2021 a 2023, Kaspersky fue socio del consorcio del proyecto de la UE DeStalk, cofinanciado por el Programa de Derechos, Igualdad y Ciudadanía de la Unión Europea. Los cinco socios del proyecto que formaron el consorcio reunían la experiencia de la comunidad de seguridad de TI, las organizaciones de investigación y de la sociedad civil y las autoridades públicas. Como resultado, el proyecto DeStalk formó a un total de 375 profesionales que trabajan directamente en servicios de apoyo a las mujeres y programas para agresores, así como a funcionarios de las autoridades públicas sobre cómo abordar eficazmente el stalkerware y otras formas digitales de violencia de género para crear conciencia pública sobre la violencia digital y el stalkerware.

Como parte del proyecto, Kaspersky desarrolló un curso de aprendizaje en línea sobre ciberviolencia y stalkerware dentro de su Kaspersky Automated Security Awareness Platform, una plataforma de formación de microaprendizaje en línea disponible de forma gratuita a la que se puede acceder en cinco idiomas diferentes. Hasta la fecha, más de 130 profesionales han realizado el curso de aprendizaje en línea y otros 80 participan actualmente. Pese a que el proyecto DeStalk ha terminado, el curso en línea sigue disponible en el sitio web del proyecto DeStalk https://www.work-with-perpetrators.eu/destalk.

En junio de 2022, Kaspersky lanzó un sitio web dedicado a TinyCheck para difundir más información sobre la herramienta. TinyCheck es una herramienta gratuita, segura y de código abierto que pueden utilizar organizaciones sin ánimo de lucro y unidades policiales para ayudar a las víctimas del acoso digital. La herramienta se creó en 2020 para comprobar la presencia de stalkerware en los dispositivos y monitorear aplicaciones sin que el autor se enterara del control. No requiere instalación en el dispositivo del usuario porque funciona de forma independiente para evitar que un acosador la detecte. TinyCheck escanea el tráfico saliente de un dispositivo mediante una conexión Wi-Fi normal e identifica las interacciones con fuentes conocidas, como los servidores relacionados con el stalkerware. TinyCheck también se puede utilizar para comprobar cualquier dispositivo en cualquier plataforma, incluidos iOS, Android o cualquier otro sistema operativo.

¿Crees que eres víctima de stalkerware? Aquí tienes unos consejos...

Tanto si eres víctima de stalkerware como si no, aquí tienes algunos consejos para protegerte mejor:

- Protege tu teléfono con una contraseña segura que nunca debes compartir con tu pareja, amigos o colegas.
- Cambia las contraseñas de todas tus cuentas periódicamente y no las compartas con nadie.
- Descarga aplicaciones únicamente de fuentes oficiales, como Google Play o la App Store de Apple.
- Instala una solución de seguridad de TI fiable como Kaspersky para Android en los dispositivos y escanéalos con regularidad. Sin embargo, en el caso de un stalkerware ya esté instalado, esto solo debe hacerse después de que se haya evaluado el riesgo para la víctima, ya que el infractor puede detectar el uso de una solución de ciberseguridad.

Las víctimas de acoso pueden ser víctimas de un ciclo mayor de abuso, incluso físico.

En algunos casos, se notifica al agresor si su víctima escanea el dispositivo o elimina una aplicación de stalkerware. Si esto sucede, puede provocar un agravamiento de la situación y una agresión mayor. Por eso es importante proceder con cautela si crees que estás siendo objetivo de un acosador.

- **Ponte en contacto con una organización de apoyo local:** para encontrar una cerca de ti, consulta el Sitio web de la Coalición Contra el Stalkerware.
- **Mantén un ojo abierto a las siguientes señales de advertencia:** pueden incluir una batería que se agota rápidamente debido a aplicaciones desconocidas o sospechosas que agotan la carga, o aplicaciones recién instaladas con acceso sospechoso para usar y rastrear tu ubicación, enviar o recibir mensajes de texto y otras actividades personales. Comprueba también si la configuración de «fuentes desconocidas» está habilitada, ya que puede ser una señal de que se ha instalado software no deseado de una fuente externa. Sin embargo, los indicadores anteriores son circunstanciales y no indican la presencia inequívoca de stalkerware en el dispositivo.
- **No intentes borrar el stalkerware, cambiar la configuración ni manipular tu teléfono:** esto podría alertar al posible agresor y provocar un agravamiento de la situación. También corres el riesgo de borrar datos o pruebas importantes que podrían utilizarse en un proceso judicial.

Para obtener más información sobre nuestras actividades contra el stalkerware o cualquier otra solicitud, escríbenos a: ExtR@kaspersky.com.

La Coalición contra el Stalkerware se fundó en noviembre de 2019 como respuesta a la creciente amenaza creada por el stalkerware. La Coalición busca combinar la experiencia de sus socios en el ámbito de la asistencia a los supervivientes de violencia doméstica con el trabajo con la persona que ha perpetrado el abuso y la defensa de los derechos digitales. Todos los miembros tienen el firme compromiso de luchar contra la violencia doméstica, el acoso y el acecho abordando la utilización de stalkerware y creando conciencia pública sobre este problema.

Coalición contra el Stalkerware:
https://stopstalkerware.org

TinyCheck:
https://tiny-check.com

Coalition Against Stalkerware

TinyCheck®

Noticias sobre ciberamenazas: www.securelist.lat
Noticias de seguridad: business.kaspersky.com
Seguridad para PYMEs:
www.kaspersky.es/small-to-medium-business-security
Seguridad para grandes empresas:
www.kaspersky.es/enterprise-security

www.kaspersky.es

kaspersky