

BIBLIOTECA POPULAR DE CULTURA LIBRE

CUIDADOS DIGITALES EN INTERNET





LABORATORIO POPULAR
DE MEDIOS LIBRES
PRESENTA:

BIBLIOTECA POPULAR DE CULTURA LIBRE

CUIDADOS DIGITALES EN INTERNET

Talleres en Casa de los Pueblos "Samir Flores"
Octubre 2023

Cuidados Digitales en Internet

Laboratorio Popular de Medios Libres
Biblioteca Popular de Cultura Libre
2024

Foto de Portada exterior

Taller en Acteal, Chiapas, México.

Foto de Portada interior

Taller de Archivo Digital en
Casa de los Pueblos Samir Flores

Textos y Contenido

Armando Gómez Martín
Chasqui Camilo

Diseño y diagramación

Chasqui Camilo

laboratoriodemedios.org
contacto@yanapak.org

La impresión de esta primera edición fue posible gracias al apoyo de:



The Fleets of New Spain: Delving into three centuries of socioeconomic history through Artificial Intelligence. Centro de Investigación en Humanidades Digitales, Universidad de Lancaster, UK - CIESAS, Mexico



Esta obra está bajo una Licencia Creative Commons Atribución-NoComercial-CompartirIgual 4.0 Internacional.

ÍNDICE

- Saludo a la lectora (pág. 6)
- Interconectadas (pág. 7)
- ¿Qué es una vulnerabilidad? (pág. 10)
- La Otra Vulnerabilidad: Nosotras (pág. 11)
- ¿De quiénes nos cuidamos? (pág. 13)
- Buenas prácticas y cuidados digitales en Internet (pág. 16)
- Buenas Prácticas y cuidados digitales en Celulares (pág. 44)
- Conoce los distintos tipos de ataques (pág. 56)
- Evalúa los riesgos y construye protocolos de seguridad (pág. 67)
- Busca y construye alternativas (pág. 70)
- Glosario (pág. 72)
- Ligas de interés (pág 83)





“Pero compartir no es inmoral –es un imperativo moral. Sólo aquellos que están cegados por la codicia se negarían a hacerle una copia a un amigo.”

Aaron Swartz

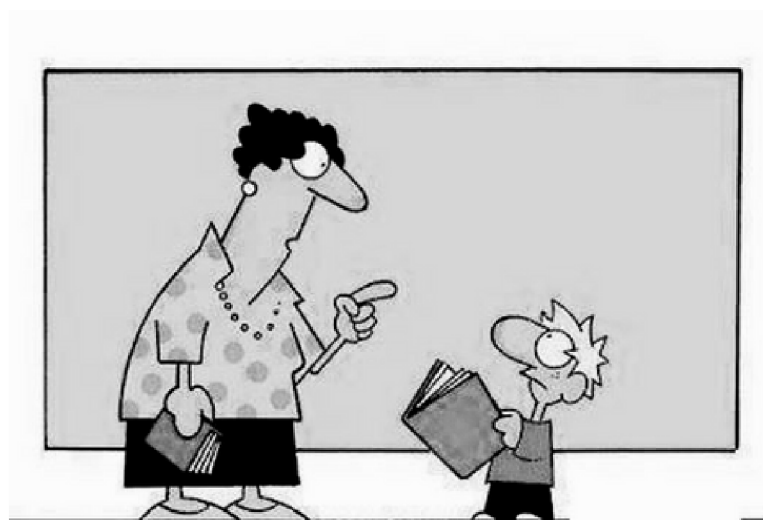
Manifiesto por la Guerrilla del Acceso Abierto

“Manténganse vivos, no tienen idea de lo importante que son y lo importante que se volverán todos y cada uno de ustedes. Las máquinas siguen avanzando... Skynet está preparando algo, pero la resistencia esta preparando algo más grande... Si están escuchando esto, ustedes son la resistencia”

John Connor

Copia y difunde

**LABORATORIO
POPULAR
DE MEDIOS
LIBRES**



Se llama leer.
Es la forma en que la gente instala
nuevo software en su cerebro

SALUDO A LA LECTORA

El texto que ahora sostienes en tus manos es el fruto de la sistematización del trabajo, experiencias y conocimientos que otras han compartido con nosotras, desde que decidimos iniciar la promoción (hace algunos años ya) de la autonomía técnica en las distintas comunidades que utilizan la comunicación como una herramienta para la defensa del territorio.

En este recorrido no nos hemos encontrado con la academia, si no por el contrario, nuestra escuela ha sido el conocimiento popular que vive en la boca, mente y corazón de cada una de las valientes que se han decidido a mantener un proyecto de comunicación autónoma y ejercer su derecho a la comunicación. Esa sabiduría es la que humildemente intentamos plasmar en el texto en que se zambullirán en unos momentos.

Ante la creciente centralización, privatización y uso no consentido de nuestra data personal en Internet, creemos fundamental comenzar a cuestionarnos la propiedad de las plataformas e infraestructuras que actualmente sostienen nuestras comunicaciones digitales y, para ello ponemos a disposición en un lenguaje sencillo, los conocimientos que hemos podido compilar con respecto a las **cuidados digitales en internet** en este tercer cuadernillo de la *Biblioteca Popular de Cultura Libre*.

Encontrarás a lo largo de este viaje algunos códigos QR , asegúrate de tener contigo un celular con una app que te permita leerlos, ya que te llevarán a varias profundas e interesantes informaciones adicionales.

Si durante tu recorrido aparece una palabra que no conoces o te parece extraña, no dudes en consultar el **glosario** al final del manual para aclarar su significado. En éste hemos intentado explicar de manera sencilla diversos términos técnicos que a veces pueden resultar confusos.

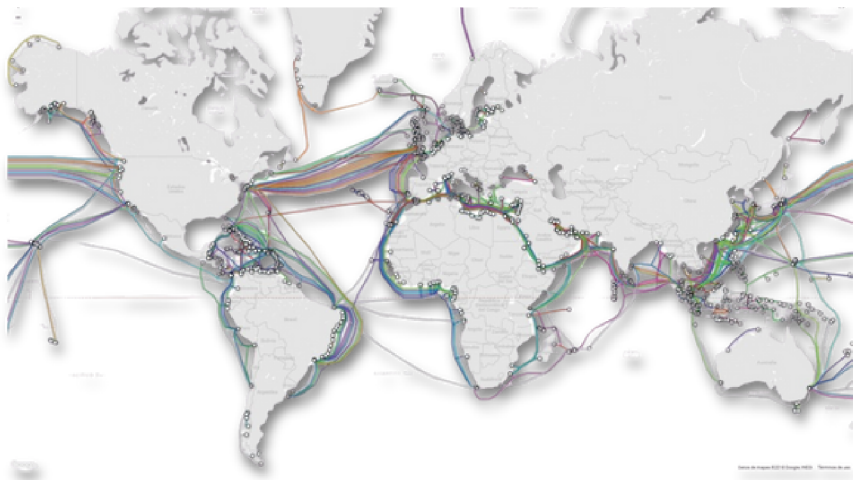
Esperamos que sea de tu agrado y por favor tómate la libertad de subrayar, dibujar o escribir sobre este cuadernillo. Abrazos.

No odies a los medios, siémbrales libres

INTERCONECTADAS

En la actualidad las interacciones con dispositivos y redes digitales son **mayores cada día** y ocupan parte importante de nuestras relaciones humanas. A través de ellas hacemos todo tipo de cosas: vemos video para informarnos o entretenernos, escribimos textos de manera colaborativa, hacemos deporte y controlamos nuestra salud, podemos aprender algún instrumento musical o hacer un post-grado en una universidad extranjera y, por supuesto las utilizamos para revisar chats, redes sociales y las distintas herramientas que usamos para comunicarnos unas con otras.

La velocidad y magnitud con las que ha ocurrido la revolución del internet han superado la capacidad de la sociedad y de los gobiernos para llevar a cabo un debate responsable y crítico sobre esta nueva tecnología. Este debate sería fundamental para arrojar luz sobre los posibles efectos, tanto positivos como negativos, de su implementación masiva en la sociedad. El **artículo 17 de la Declaración Universal de Derechos Humanos** reconoce el derecho a la privacidad, a que toda persona debe ser protegida contra injerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio o su correspondencia. Sin embargo, las grandes empresas de internet violan constantemente este principio en el mundo digital.



Fibra óptica submarina que es en la actualidad la red que mayoritariamente conecta al mundo y que esta en manos de empresas privadas

FIBRA ÓPTICA SUBMARINA

A lo largo de los mares del mundo se extienden cables de fibra óptica que conectan continentes y permiten la transmisión de datos a grandes distancias. Estos cables son fundamentales para el funcionamiento de internet ya que transportan la información de manera eficiente y segura.

No existe un acuerdo universal sobre cómo funciona la privacidad en Internet y aún así el modelo de negocios en línea se basa principalmente en la recopilación y el aprovechamiento del enorme rastro digital que dejamos mientras navegamos por la web. Cada clic, búsqueda o interacción en línea deja una **huella digital** que las empresas recopilan, comparten y utilizan para comprender mejor nuestros intereses, comportamientos y preferencias. Esta información, invaluable para las empresas de publicidad, se utiliza para personalizar anuncios de ventas y campañas políticas con extrema precisión.

Esta práctica no está exenta de controversia. A medida que la recopilación de datos se ha vuelto más sofisticada y masiva no existen regulaciones nacionales o internacionales que sancionen o den marcos regulatorios, dejando a las empresas con un gran margen de libertad en el mundo digital. Por este motivo han surgido preocupaciones sobre la privacidad y la ética. Algunas empresas han sido acusadas de utilizar métodos poco éticos para obtener información personal, incluso violando sus propias políticas de protección de datos. Mark Zuckerberg, el CEO de Facebook, ha comparecido en más de una ocasión ante instancias judiciales internacionales para reconocer estas prácticas cuestionables.

EL CASO FACEBOOK- CAMBRIDGE ANALYTICA

Cambridge Analytica alardeó de tener 5.000 datos específicos sobre cada votante estadounidense. Podía determinar el tipo de personalidad de cada votante y luego dirigirle mensajes con noticias falsas diseñadas para influir en su comportamiento. La fuente más importante de datos era Facebook. A través de la aplicación de un tercero, Cambridge Analytica obtuvo indebidamente datos de hasta 87 millones de perfiles de Facebook, que incluían actualizaciones de estado, indicaciones de “me gusta” e incluso mensajes privados.

Sin duda la era digital nos ha proveído de herramientas que proporcionan ayuda para resolver problemas y ejecutar actividades de todo tipo, facilitando la vida humana. Sin embargo, también han crecido los riesgos y peligros en el uso y abuso de esta tecnología. Al igual que en la vida material, los riesgos son múltiples y en continuo desarrollo. El saber cuidarnos de manera colectiva y personal es uno de los objetivos de este breve escrito.

Empezaremos diciendo que: **no hay internet seguro, pero sí podemos reducir el nivel de riesgo y vulnerabilidad de su uso con buenas prácticas.**

El internet actual es controlado por grandes empresas que no son ejemplo de privacidad o seguridad digital hacia sus usuarias a quienes las ve más como ingresos. A esto se suma el número de ciberataques, fraudes, estafas, secuestros, acosos, espionajes, robos que siguen creciendo día con día; realizados por gobiernos, empresas y gente malintencionada.

Por eso es importante hablar sobre la seguridad de las comunicaciones y la necesidad de cuidarnos en ellas mediante buenas prácticas. Si los gobiernos y las instancias internacionales no han logrado regular adecuadamente, dejando en manos privadas el mundo digital, se hace necesario que nos capacitemos colectivamente en las nuevas herramientas y sus riesgos. Es crucial asumir de manera consciente la interacción con los dispositivos y dejar de ser simples usuarias para convertirnos en administradoras de nuestro propio destino.

súbete, vamos a cambiar las configuraciones de privacidad y seguridad



No hay internet seguro, pero si podemos reducir el nivel de riesgo y vulnerabilidad con buenas prácticas.

La privacidad es un derecho importante y un habilitador esencial de la autonomía, dignidad y libertad de expresión de un individuo. Pero la privacidad en línea está bajo una presión constante de ser vulnerada y es necesario que tomemos cartas en el asunto.

¿QUÉ ES UNA VULNERABILIDAD?

Pero... ¿Qué es una vulnerabilidad?, ¿Cuáles son los riesgos que tengo en el uso del internet y dispositivos digitales?

Una vulnerabilidad es un error o fallo que representa una posibilidad de poner en riesgo los datos que hemos confiado en alguna computadora.

Cuando un dispositivo móvil o una computadora tiene un error en su construcción física, se le conoce como vulnerabilidad de hardware. Por otro lado, cuando una de sus aplicaciones instaladas presenta un fallo en su código que puede ser explotado para causar daño a las usuarias, se le denomina vulnerabilidad de software. En ambos casos, la vulnerabilidad representa una posibilidad de que se viole el derecho a la privacidad y se roben tus datos.

El software, también conocido como aplicaciones o programas, es creado por seres humanos que se esfuerzan por hacerlo lo mejor posible. Sin embargo, aún así, existen posibilidades de cometer errores durante su desarrollo.

Imagina que tienes una puerta en tu casa que no cierra bien. Esa puerta sería una vulnerabilidad, ¡porque alguien podría entrar sin permiso! Del mismo modo, en el mundo digital hay "puertas" que no están del todo seguras y pueden ser aprovechadas por personas malintencionadas.

Es importante saber que estas vulnerabilidades pueden tener diferentes impactos. Algunas podrían permitir que las "malvadas" accedan a tu información personal, mientras que otras podrían causar problemas en el funcionamiento normal de tus dispositivos.

Para proteger nuestra casa ponemos cerraduras más fuertes en las puertas o conseguimos un perro que cuide el hogar. En el mundo digital, también podemos tomar medidas, como instalar actualizaciones de seguridad en nuestros dispositivos y aprender sobre buenas prácticas en línea.

LA OTRA VULNERABILIDAD: NOSOTRAS

Pero la seguridad digital abarca más que simplemente protegerse contra vulnerabilidades del software o ataques externos; también implica reconocer y abordar las vulnerabilidades que pueden surgir de nuestras propias acciones en línea. Estas malas prácticas pueden convertirse en puntos débiles significativos que los agentes malintencionados pueden aprovechar para acceder a nuestra información personal o comprometer nuestra seguridad en línea.

En realidad, una de las principales vulnerabilidades en internet somos nosotras mismas, las usuarias. En muchos casos, compartimos de manera indiscriminada y sin mucha consideración una gran cantidad de información personal en redes sociales y otros sitios en línea. Desde detalles sobre nuestra vida cotidiana hasta fotografías de eventos importantes, tendemos a publicar una amplia gama de información sin realmente pensar en las posibles repercusiones.

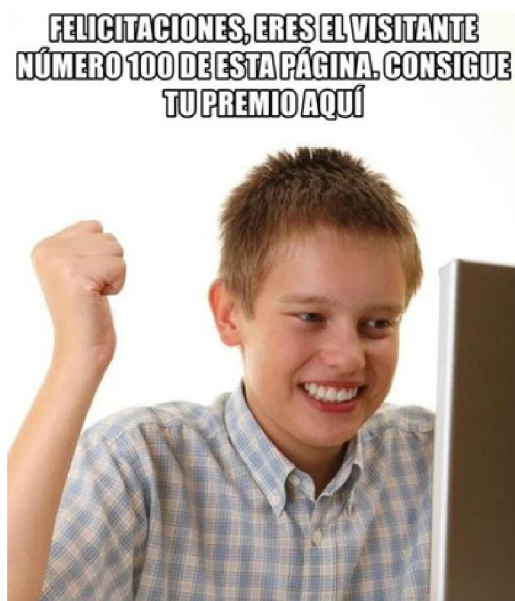


Esto nos expone a una serie de riesgos, incluido el robo de identidad, donde los delincuentes pueden usar la información que compartimos para suplantar nuestra identidad y cometer fraudes financieros u otros delitos en nuestro nombre. Las depredadoras en línea y las acosadoras pueden aprovechar la información que compartimos para rastrearnos, acosarnos o amenazarnos. Incluso algo tan aparentemente inofensivo como publicar una foto en la playa puede poner en riesgo nuestra seguridad personal si cae en manos equivocadas.

No solo estas malas prácticas nos ponen en riesgo, sino también nuestras emociones y aspectos psicológicos, que constantemente son explotados para atacarnos, en lo que se conoce como **ingeniería social**. Esta táctica implica manipular y engañar a las personas para obtener información confidencial o acceso no autorizado a sus sistemas informáticos. A diferencia de los ataques tradicionales, que aprovechan las vulnerabilidades de software, la ingeniería social se basa en encontrar puntos débiles en la confianza y la humanidad de las víctimas.

Imagina recibir una llamada telefónica de alguien que se identifica como representante de una empresa de servicios públicos. Te informan que ha habido un error en tu última factura y que necesitan verificar algunos detalles de tu cuenta para corregirlo. A pesar de que la llamada parece legítima y proporcionan información precisa sobre tu dirección y consumo de servicios, en realidad se trata de un intento de ingeniería social. La estafadora está tratando de obtener información confidencial, como tu número de seguridad social o detalles de pago, aprovechando tu confianza en la supuesta autoridad de la empresa de servicios públicos.

Nuestras propias acciones y prácticas en línea pueden representar una fuente significativa de vulnerabilidades en materia de seguridad digital. Es esencial estar conscientes de estas malas prácticas y tomar medidas proactivas para proteger nuestra seguridad y privacidad en línea. La educación y la conciencia sobre nuestras propias vulnerabilidades son fundamentales para evitar caer en trampas o ser víctimas de ataques cibernéticos.



¿DE QUIÉNES NOS CUIDAMOS?

En la ciberseguridad se le llama **agente malicioso/a**, agente de intrusión, o atacante a quienes ocupan vulnerabilidades para atacar a un tercero. Hay quienes confunden el término hacker con el de agente maliciosa o cibercriminal.

La palabra **hacker** tiene sus orígenes en el Instituto Tecnológico de Massachusetts (MIT), donde se utilizaba para describir a estudiantes que tenían un gran talento y pasión por la resolución de problemas informáticos. Las hackers actuales son en su mayoría autodidactas y se dedican a explorar y mejorar los sistemas informáticos de manera creativa y constructiva, su conducta ética es la que determina si son buenas o malas personas.

Por otro lado, las **agentes maliciosas** son personas que trabajan de manera independiente, para empresas o estados para atacar y espiar por alguna ganancia económica: las **cibercriminales**.

En el caso de comunicadoras y defensoras populares el análisis de riesgo de su ciberseguridad no sólo pasa por el definir e identificar a las "agentes maliciosas", es muy importante sumar en su análisis **los servicios de la red y su infraestructura tanto del Estado como de empresas privadas**.

Es fundamental conocer quién provee la infraestructura de red, los servidores y servicios que utilizamos en nuestro día a día. Comprender las políticas bajo las cuáles operan estas empresas y su relación con el estado, ya que ésto puede tener implicaciones importantes en términos de privacidad y confidencialidad.

RUSIA, EL MAYOR SOLICITANTE DE ELIMINACIÓN DE CONTENIDO DE GOOGLE

En el primer semestre de 2021, el último informe disponible de Transparencia de Google, Rusia presentó cerca de 19.000 solicitudes para eliminar más de 200.000 elementos. Los gobiernos de todo el mundo pueden dirigirse a Google con lo que quieren que la empresa elimine de sus plataformas en la web.

La venta y el intercambio de datos personales han generado debates cruciales sobre la necesidad de implementar regulaciones más estrictas para proteger la privacidad de las usuarias en línea, especialmente para defensoras de derechos humanos. En este escenario, los estados también han aprovechado este vacío legal para establecer equipos de monitoreo en línea, encargados de detectar posibles amenazas a sus intereses. Estos equipos a menudo descritos como aparatos represivos digitales, cuentan con el respaldo de las grandes empresas tecnológicas, con las cuales intercambian información.

Este vínculo entre los estados y las “Big Tech” plantea serias preocupaciones sobre la privacidad y la libertad de expresión. La colaboración entre estas entidades podría conducir a una vigilancia excesiva y a la represión de la disidencia en línea, socavando el derecho universal a la libre expresión.

En América Latina, el derecho a la comunicación ha surgido como una herramienta efectiva en las luchas de los pueblos, que históricamente se han enfrentado a la complicidad entre los estados, los medios de comunicación y las empresas que buscan explotar los recursos naturales en sus territorios. El poder económico y político ejercido por las multinacionales, ya sean de origen canadiense, estadounidense, europeo, chino u otro, no tiene comparación con el poder de un gobierno local o una comunidad organizada. Esta disparidad de fuerzas se agrava cuando se suma a la ecuación la denunciada concentración de la propiedad de los medios de comunicación en el continente.



No solo nos cuidamos del ciber ladrón,
también nos cuidamos del ciber control y del ciber policía.

Por ello es que justamente internet ha sido el espacio donde se han volcado innumerables esfuerzos de comunicación independiente en la región. La comunicación comunitaria en el mundo digital no sólo es un medio para informar, sino también para empoderar a las comunidades y promover el cambio social. Al permitir que las voces marginadas y excluidas sean escuchadas, se construye una narrativa alternativa que desafía las estructuras de poder existentes y abre espacio para la resistencia y la transformación social. El derecho a la privacidad en línea se convierte en un elemento crucial para proteger la seguridad y la integridad de quienes participan en estos esfuerzos de comunicación comunitaria, frente a posibles represalias o ataques de aquellos que buscan silenciar su voz.

Es esencial que la adopción de internet y las TIC (tecnologías de la comunicación y la información) se realice desde una perspectiva crítica. Esto nos permitirá reconocer tanto las ventajas como los riesgos que conlleva el uso de estas herramientas. Es imperativo que las comunidades adquieran la capacidad de realizar análisis de riesgos que les permitan adoptar medidas de cuidado digital y establecer comunicaciones seguras. Esto les facultará para ejercer su derecho a la comunicación en la defensa de su territorio.

El mundo digital actual es hostil porque se mueve por intereses capitalistas, su motor es el hambre de riqueza material por encima del bien común. Es muy importante que colectivamente aprendamos a reconocer cómo las mismas viejas prácticas y actores del mercado se han trasladado al internet, inundándolo y transformándolo por asalto.

Pero al igual que en el mundo real, existen alternativas que se construyen desde abajo; podemos habitar el ciberespacio en las grandes granjas de ordenadores de mega corporaciones o en los servidores autónomos del ciberactivismo, donde quienes mantienen esos servicios lo hacen para cuidar de nosotras y nuestros datos. Recordemos que las herramientas del amo no serán las que nos liberarán.

Esta guía es una invitación a reflexionar colectivamente sobre nuestra realidad, para reconocer de quiénes y cómo nos cuidamos, quienes son nuestras aliadas y cómo podemos construir un entorno digital más seguro para todas.

BUENAS PRÁCTICAS Y CUIDADOS DIGITALES EN INTERNET

CONSIDERACIONES PREVIAS

Creemos que no existe un manual único de seguridad digital que pueda resolver todas las adversidades. Cada grupo social que interactúa en línea, ya sea niñas, adolescentes, adultas jóvenes, adultas mayores, personas con discapacidades, comunidades LGBTQ+, comunidades indígenas, trabajadoras de la salud, profesionales de la educación, entre otras, tienen necesidades y desafíos específicos en cuanto a seguridad y cuidado digital. Por ejemplo, las niñas pueden requerir pautas para proteger su privacidad en redes sociales y evitar el acoso en línea, mientras que las adultas mayores pueden necesitar consejos para detectar estafas y fraudes en Internet.

Cada manual de seguridad y cuidado digital debe ser adaptado a las características y necesidades de cada grupo social. Esto implica considerar factores como el nivel de alfabetización digital, la experiencia en tecnología, las barreras lingüísticas, entre otras. Además, estos manuales deben ser actualizados constantemente para mantenerse al día con los cambios en la tecnología y las nuevas amenazas en línea.

En la actualidad las organizaciones sociales y movimientos populares deben asumir esta responsabilidad de manera colectiva, integrando grupos o dinámicas de trabajo para enfrentar los retos de la seguridad digital para sus colectividades. Tener espacios para platicar y capacitarse sobre esos temas. Promover la autonomía a la par del uso consciente de las herramientas digitales se hace fundamental en el día actual.

Los manuales avanzados de seguridad que hemos podido revisar no sólo se centran en prevenir y defenderse de ataques externos, sino que también consideran la posibilidad de amenazas internas. Por ejemplo, estos manuales pueden instruir a las empleadas o estudiantes a estar atentos a comportamientos sospechosos entre sus compañeras de trabajo o colegas de clase, como intentos de sabotaje, robo de información confidencial o comportamiento potencialmente peligroso.

La seguridad digital para defensoras, comunicadoras o activistas, se esfuerza por mantener seguras y protegidas a las personas en línea mientras continúan su lucha por la justicia y el cambio social. Esto requiere una combinación de conciencia, educación y el uso de herramientas y estrategias de seguridad digital colectivas efectivas para hacer frente a las diversas amenazas que enfrentan en el mundo digital.

Las defensoras de derechos, comunicadoras y activistas se esfuerzan por buscar lugares seguros para almacenar archivos, comunicaciones encriptadas para garantizar su privacidad o, cómo prevenir el acoso y la persecución para protegerse de campañas de odio entre otras formas de violencia, tanto antiguas como emergentes, que pueden manifestarse en el mundo digital.

Pero toda esta complejidad no es necesaria que la afrontemos solas, no somos las únicas en el páramo digital, para estos desafíos existen los laboratorios hacker, o hacklabs; ejemplos vivos de entornos comunitarios donde se comparte conocimiento tecnológico en un ambiente de igualdad y colaboración. En estos espacios, se organizan talleres y capacitaciones constantes y variadas, fomentando el aprendizaje continuo y el intercambio de habilidades. Además, estos espacios pueden adoptar diferentes nombres y estar vinculados a diversas organizaciones, como las comisiones de comunicación o prensa dentro de movimientos sociales o colectivos.

Es crucial pensar en la seguridad como un aspecto a considerar en los entornos en los que nos movemos y en las formas en que nos relacionamos en Internet. Esto implica analizar de manera colectiva los contextos en los que operamos y adoptar medidas proactivas en común para proteger nuestra privacidad y seguridad en línea.

Es importante destacar que existen alternativas a las hegemonías capitalistas, donde se privilegia lo comunitario sobre lo individual.

Al igual que el software libre, que promueve el acceso abierto y la colaboración en el desarrollo de herramientas tecnológicas, también existen espacios de trabajo colaborativo para otras tecnologías, concebidas y construidas en colectivo para el beneficio común. Esta actitud rebelde ante el capitalismo se centra en el compartir y en pensar en el bienestar colectivo por encima del beneficio individual.

En resumen, la creación de espacios colectivos y la adopción de una actitud colaborativa y solidaria son fundamentales para enfrentar los desafíos de seguridad digital en la era de la “sociedad de la información”. Al promover el intercambio de conocimientos y la colaboración en la construcción de soluciones tecnológicas, podemos avanzar hacia un mundo digital más inclusivo, equitativo y seguro para todas.

Dicho esto, veamos pues algunos consejos prácticos para el uso de servicios en internet ya sean privados o en servidores libres, que podemos implementar, compartir o usar simplemente para iniciar una charla sobre seguridad y autocuidados digitales.



“Ser consciente de las vulnerabilidades es ya la mitad de la seguridad”

Escuchado en un Hackomún

RELACIÓN ENTRE SOFTWARE LIBRE Y SEGURIDAD DIGITAL

Empezaremos diciendo que para mejor certeza de tu seguridad digital se recomienda el uso de sistemas operativos y aplicaciones (software) libres o de código abierto. Sistemas Operativos como GNU-Linux y sus distribuciones más relevantes: Debian, Ethertics, Linux Mint, Ubuntu, Tails, Parrot son buenas alternativa para PC.

Para el caso del móvil y tabletas son pocos los sistemas operativos que ofrecen el mercado, la hegemonía es Android que si bien es un desarrollo basado en Linux es controlado por Google. Otro sistema es iOS de MacOs para los teléfonos Apple. Últimamente han salido nuevos sistemas operativos para telefonía móvil, como los lanzados por HUAWEI y Microsoft. Pero **son sistemas operativos cerrados y controlados**. Lo que si permiten Android y MacOs es un extenso surtido de aplicaciones de Software Libre o de Código abierto, que se abrevia FOSS (Free and Open Source Software). En el caso de Android puedes encontrar un extenso repositorio en F-Droid que es un repositorio de softwares para Android.

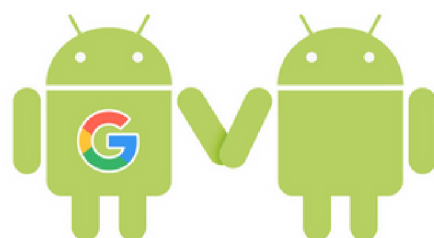
Puedes descargarlo directamente de su página <https://f-droid.org/>

DESCARGA PROGRAMAS O APLICACIONES DE F- DROID

F-Droid es una tienda de aplicaciones independiente y de origen comunitario para Android que es completamente gratuita y de código abierto. En F-Droid puedes navegar por más de 1200 aplicaciones, buscar e instalar aplicaciones de repositorios creados o crear tu propio repositorio



Aunque Android nace de un código abierto, es un Frankenstein de Google por lo que tiene candados muy fuertes que impiden que las usuarias puedan tomar el control de su teléfono. (A veces hay alternativas como el rooteo). En Android y demás sistemas operativos y apps privativas no se puede tener esa certeza de sus medidas de seguridad o qué datos recopilan, pues no sabemos cómo funcionan dentro de nuestros teléfonos.



En nuestras comunidades, el uso de Linux aún no es común, a pesar de la necesidad de promoverlo. La mayoría de los equipos y dispositivos siguen siendo privativos. **Linux ha sido diseñado con un enfoque en la protección de datos y la privacidad de la usuaria**, lo cual es fundamental en la era digital en la que vivimos. El interés principal de los sistemas operativos privados que usamos constantemente es el beneficio comercial a toda costa. Linux se preocupa por brindar una experiencia segura y confiable a sus usuarias.

Además, cuenta con un amplio conjunto de herramientas y características de seguridad integradas, como firewalls, sistemas de detección de intrusiones y cifrado de datos. A diferencia de otros sistemas operativos que recopilan y comparten datos personales sin el consentimiento de la usuaria, Linux respeta la privacidad y ofrece opciones para controlar la recopilación y el uso de datos.



chromeOS



Como dijimos anteriormente, a veces los programas pueden contener errores en su creación, lo cuál representa una vulnerabilidad para tu seguridad. Por ese motivo es que constantemente se realizan actualizaciones en el mundo digital. Estas actualizaciones son pequeños parches que arreglan vulnerabilidades que fueron descubiertas después que el software se lanzó al público. En Linux la acción de actualizar es muy sencilla y siempre es gratuita.

Muchas veces cuando no queremos pagar por un software privativo, ocupamos la piratería, lo cuál representa un alto riesgo para nuestra seguridad, no sólo porque no podrás actualizar el programa “crackeado”, sino porque por lo general estos programas **contienen virus o malware en su interior**. Es mucho mejor usar alternativas libres y seguras.

Al utilizar software libre tenemos la certeza de que en el código, al interior del programa, no hay nada que pueda dañarnos. Esta característica es una gran ventaja que aumenta nuestra seguridad digital de manera significativa. Al ser de código abierto, cualquier persona puede examinar el código y detectar posibles vulnerabilidades o malwares ocultos. Esto nos brinda tranquilidad y confianza al utilizar software libre, sabiendo que estamos protegidas contra posibles ataques y que nuestras actividades en línea están respaldadas por una comunidad de expertos comprometidos con la seguridad digital.

También existen muchas ventajas a la hora de manejar nuestra **huella o rastro digital**, porque podemos acceder a los metadatos y modificarlos con mayor facilidad. Esto es especialmente útil cuando se trata de proteger nuestra privacidad y asegurarnos de que la información que compartimos en línea no se utilice en nuestra contra.

¿QUÉ SON LOS METADATOS?

Cada vez que hacemos una foto con teléfono, una tablet, una cámara digital; el archivo de la imagen contiene unos datos (metadatos) que revelan la fecha, hora y lugar en la que fue tomada la fotografía, el modelo del dispositivo, la versión del sistema operativo y otros parámetros. Toda esta información la usan y comparten con terceros las empresas para su diseño de productos.



El uso de sistemas libres donde existe muchísima menos vulnerabilidad en su código, más la capacidad de gestionar nuestros metadatos de manera más precisa, nos brinda la oportunidad de proteger nuestra privacidad.

Entonces siempre será recomendable optar por software y aplicaciones libres o de código abierto. Donde son comunidades auto organizadas que se nutren y se apoyan para desarrollos tecnológicos y los comparten en común. El software libre tiene 4 libertades: 1 el de estudiar el código, 2 el de usarlo, 3 el de mejorar o modificarlo y 4 el de compartir el código de manera común.

Pero ya sea que ocupemos software libre o privativo, lo primordial es que revisemos nuestras prácticas, ya que muchas veces por desconocimiento o por simple flojera de leer, somos nosotras mismas quienes entregamos información a las empresas y gobiernos.

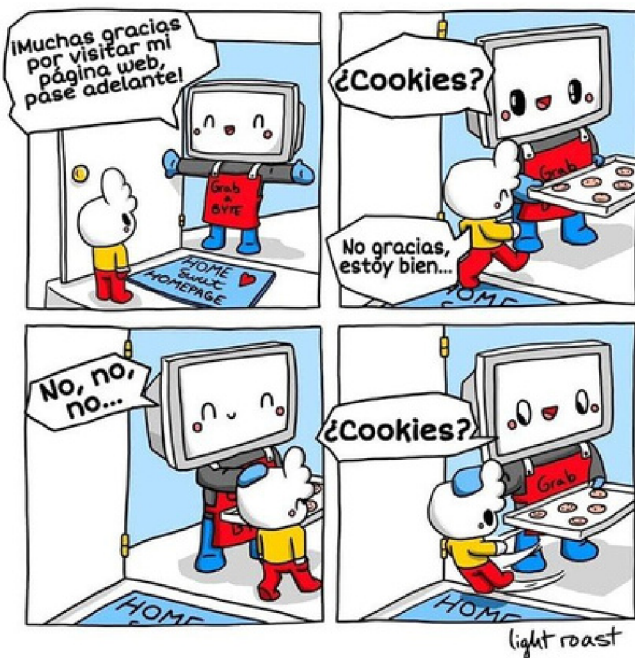
¿QUÉ SON LAS COOKIES?

Lo primero es lo primero: es importante identificar tres actores principales que trabajan juntos para rastrear a las usuarias y crear perfiles de cada una de nosotras: las empresas que buscan vender algo, las agencias de publicidad y las empresas de internet.

Entonces, averigüemos quién nos sigue en Internet desde el contexto comercial. Los gobiernos también utilizan algunas de las mismas técnicas, pero con diferentes motivaciones y condiciones legales.

Cuando navegas por un sitio web, el sitio coloca una cookie de seguimiento en tu navegador web. El navegador almacenará esa cookie en tu dispositivo. El trabajo de las cookies es recordar preferencias y configuraciones específicas cuando visitas una página web, como el idioma preferido, la ubicación geográfica o dónde diste click en el sitio web. Esto permite que la página o plataforma te “recuerde” cada vez que lo visitas, ofreciéndote una experiencia personalizada.

Los sitios web no tienen información sobre quiénes somos como tal, ya que no tenemos cuentas en ninguno de estos sitios web, pero aún así se puede adivinar tu edad, sexo, ingresos y otros detalles de hábitos de lectura y navegación.



Diversas empresas de internet pueden tener acceso a las cookies de los sitios web. Reúnen toda esa información (Big Data), la filtran y perfilan a la usuaria con decenas de criterios diferentes: edad, ingresos, hábitos de compra, sexo, ubicación, intereses, lo que sea. Posteriormente esta información es comprada por las agencias de publicidad para clasificar a los espectadores en diferentes categorías y luego ofrecen a las empresas que quieren vender algo la posibilidad de acceder a esos “ojos”.

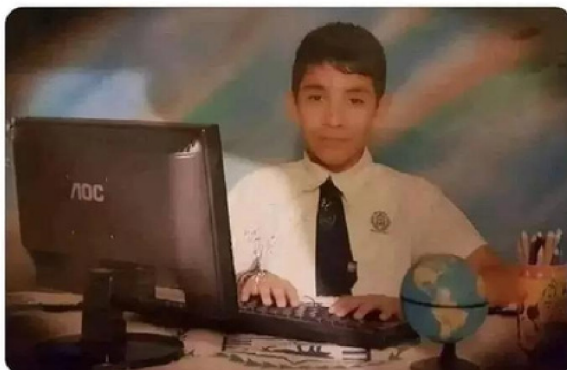
Google, Amazon, Temu, Aliexpress, TikTok, etc, recopilan información en gigantescas bases de datos y la venden a los anunciantes para orientar los anuncios. La suposición de que las cookies de seguimiento de terceros son anónimas es ampliamente discutida. Aunque la mayoría de las empresas se esfuerzan por no almacenar información que identifique directamente a una persona, los investigadores han demostrado que esto no ofrece mucha protección.

Sólo se necesitan unos pocos datos, especialmente cuando se incluye una ubicación, para rastrear un conjunto de eventos web hasta una persona real, lo que ofrece la posibilidad de seguir a esa persona real hacia atrás y hacia adelante en el tiempo.

Esta dinámica económica ofrece a cualquier proveedor de servicios digitales un fuerte incentivo para recopilar datos y mantener a las usuarias subinformadas sobre ese aspecto del servicio.

Al igual que muchos tipos de comportamiento humano (fumar, comer alimentos grasos, una mala postura), si no podemos ver un daño inmediato de nuestras acciones, tendemos a asumir que no nos están haciendo daño. La combinación de conveniencia y falta de daño aparente nos adormece en hábitos que erosionan la privacidad.

**Yo aceptando las cookies de
todas las páginas de internet a las
que accedo sin tener idea de qué
son las cookies:**



TENER CONTRASEÑAS ÚNICAS Y FUERTES

Las contraseñas son un tema clave en la seguridad digital, la autenticación juega un papel fundamental en la protección de nuestra información personal y confidencial. A medida que avanzamos en la era digital, es cada vez más importante tener contraseñas seguras para evitar posibles ataques cibernéticos.

Existen varias buenas prácticas que podemos seguir para mejorar la seguridad de nuestras contraseñas. En primer lugar, es recomendable utilizar contraseñas largas y complejas. Esto significa combinar letras **mayúsculas** y **minúsculas**, **números** y **caracteres especiales**. Cuanto más diversa sea nuestra contraseña, más difícil será para las hackers adivinarla.

Pensemos en una frase que sea fácil recordar, por ejemplo:

mi contraseña segura

Lo primero que haremos será agregar mayúsculas al inicio de cada palabra, así

Mi Contraseña Segura

A continuación reemplazaremos las algunas letras por números y la S por signo dólar:

M1 C0ntr4s3ñ4 \$36ur4

Y finalmente agregamos signos, estos pueden ser para unir las palabras o ir al final de la contraseña, así:

M1_C0ntr4s3ñ4_\$36ur4!?

Con estos simples pasos ya hemos creado una contraseña mucho más difícil de vulnerar para que uses en tu vida diaria. Muy bien! pero aún tenemos que cuidar nuestras prácticas respecto a esta contraseña que hemos creado. Por ejemplo es muy importante que no utilices la misma para todos tus servicios digitales, porque



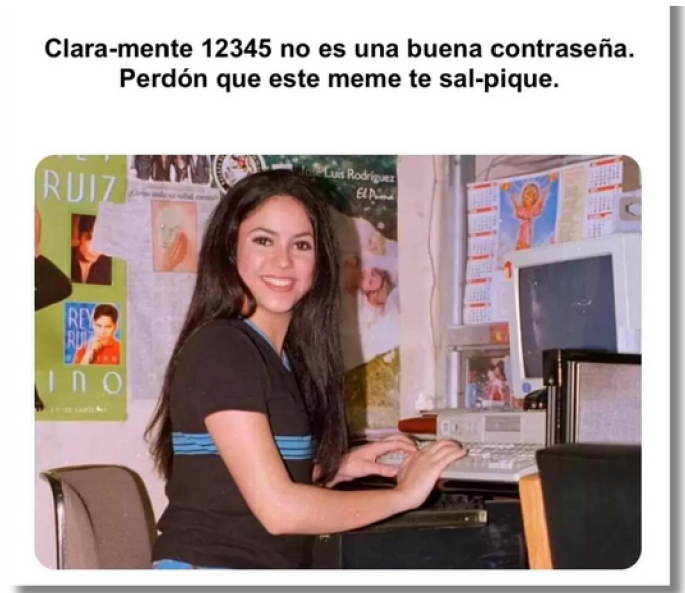
de esta manera se la pones fácil al cibercriminal, basta tener 1 contraseña tuya para tener acceso a toda tu vida. **Cada plataforma o servicio requiere de una contraseña única y robusta** para garantizar la protección adecuada.

Siguiendo nuestro ejemplo podemos agregar una palabra más a la contraseña que haga referencia a la plataforma a la que corresponde la contraseña, por ejemplo:

M1_C0ntr4s3ñ4_\$36ur4!?-f4c3b00k
M1_C0ntr4s3ñ4_\$36ur4!?-1nst4gr4m
M1_C0ntr4s3ñ4_\$36ur4!?-gm41l



- Otras recomendaciones
- No es buena idea usar solo una palabra, opta por usar frases siguiendo el ejemplo anterior.
 - Debe de tener entre 8 y 16 caracteres. Entre más caracteres es más difícil su vulneración.
 - No las compartas con otras personas, ni las dejes anotadas por ahí.
 - Cada cierto tiempo cámbialas, actualizarlas constantemente es una muy buena practica de seguridad.



Utilizar un software para almacenar las contraseñas es muy útil. Conocidos como llaveros de contraseñas, estos programas almacenan las contraseñas de nuestros servicios, evitando así la necesidad de recordarlas una por una. Esta práctica de seguridad es altamente recomendada, ya que nos permite tener contraseñas seguras y únicas para cada servicio que utilizamos. Además, estos programas suelen ofrecer funciones adicionales, como la generación automática de contraseñas fuertes y la sincronización entre dispositivos, lo que facilita aún más la gestión de nuestras credenciales.

Cada día, utilizamos una gran cantidad de servicios en línea, desde redes sociales y correos electrónicos hasta plataformas de compras y banca en línea. Cada uno de estos servicios requiere una contraseña para proteger nuestra información personal y garantizar nuestra privacidad.



KEEPASSXC: UN GESTOR DE CONTRASEÑAS LIBRE Y GRATUITO

KeePassXC es un gestor de contraseñas libre y multiplataforma, es decir funciona en Windows, Linux y Mac. Puedes descargarlo de <https://keepassxc.org/> y en el código QR te dejamos un tutorial.

- ¿Cuál es la manera más segura para guardar tus contraseñas?

- Un gestor de contraseñas.

- ¿Y por qué pusiste “guardarlas en el bloc de notas”?



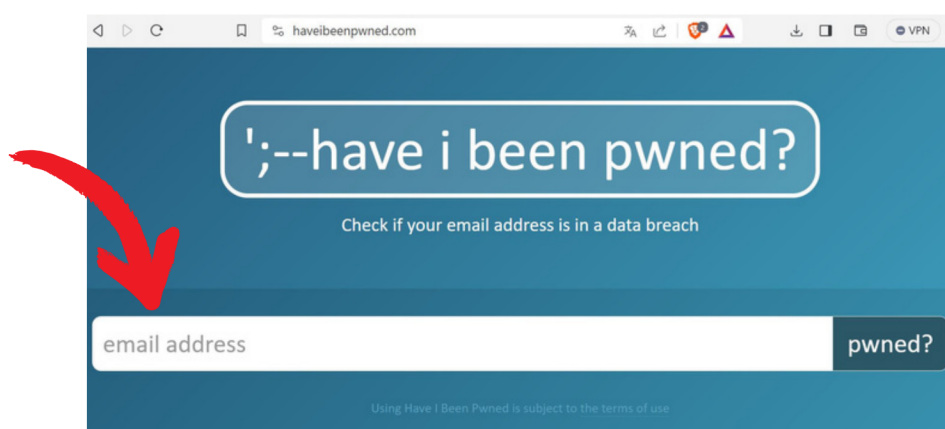
REVISA REGULARMENTE SI TU PLATAFORMA FAVORITA HA SIDO HACKEADA

Constantemente las redes sociales, los servidores de correos, los servicios de nube, etc. sufren ataques y filtraciones de datos, dónde nuestras contraseñas e información almacenada en esas plataformas quedan expuestas a agentes maliciosos. Esto sucede con una frecuencia mucho más común de lo que imaginamos y las empresas que nos dan los servicios de red no nos notifican de esto, por eso tenemos que hacerlo nosotras mismas.

Para ello recomendamos visitar la página web:



<https://haveibeenpwned.com/>



Escribe el correo que usas para ingresar a tus servicios y da click en **pwned?**. Si tu correo está en la base de datos y aparece como vulnerado, te dirá en que servicio robaron tus datos y desde cuando se sabe de esta brecha. Si es así, cambia tu contraseña en esos servicios y en tu cuenta de correo. Que haya sido vulnerada o robada no significa que ya la hayan ocupado, pero podrían hacerlo.

A veces aparecen varias cuentas en plataformas que no reconocemos, esto se debe a que por mucho tiempo no has cambiado tu contraseña y tu correo ha sido usado para crear otras cuentas... date cuenta amiga, ese correo huele a peligro.

TODO SERVICIO EN INTERNET ES UN ACUERDO DE CONFIANZA

Nada puede asegurar que no podamos ser espiadas o trazada nuestra actividad por quienes nos brindan los servicios (Google, Facebook, Amazon, etc). Las administradoras de las plataformas en internet (es decir las empleadas que trabajan en las empresas tecnológicas) tienen acceso a nuestros datos y pueden acceder a ellos de maneras que no podemos controlar. Esto significa que, aunque creamos que nuestras comunicaciones son privadas, en realidad pueden ser observadas por terceros.

Por ello es que cada vez que obtenemos una cuenta en alguna plataforma o servicio debemos firmar un acuerdo legal. En ese acuerdo se determinan cuáles son las responsabilidades del servidor antes nuestros datos, qué puede o no hacer con ellos. Informarnos de los términos del servicio es fundamental para comprender hasta qué punto entregamos nuestra información a las empresas privadas.

Yo viendo como todos se quejan de los términos y condiciones de #WhatsApp y yo le puse aceptar sin leer nada.

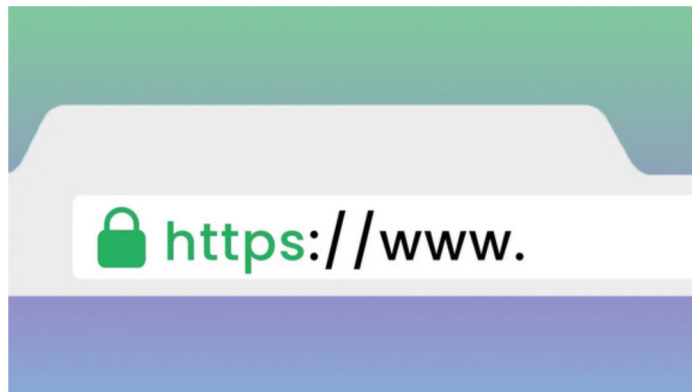


Además, es crucial considerar que estos acuerdos legales tienden a ser largos y complicados de entender, con el propósito de salvaguardar a la empresa y desalentar a las usuarias a leerlos.

De ser posible, es esencial leer detenidamente estos acuerdos y asegurarnos de comprender cada una de sus cláusulas antes de aceptarlos. De esta manera, estaremos informadas sobre cómo se utilizarán nuestros datos, quién tendrá acceso a ellos y qué derechos tenemos como usuarias.

VISITA SITIOS SEGUROS

Cuando navegas por internet es fundamental estar atenta a la seguridad que ofrecen los sitios y páginas web que visitamos, especialmente si vamos compartir información sensible en ellas, como realizar comercio electrónico. Una forma rápida y sencilla de verificar la seguridad de un sitio web es buscando el símbolo del candado en tu navegador. Este pequeño icono, generalmente ubicado en la barra de direcciones, es una señal de que estás navegando en una conexión segura.



El icono del candado indica que el sitio web que estás visitando tiene un certificado de seguridad válido. Este certificado es emitido por una autoridad de certificación y garantiza que la información transferida entre tu navegador y el sitio web está encriptada y protegida contra posibles ataques de terceros. En otras palabras, la comunicación entre tu dispositivo y el sitio web está protegida y no puede ser interceptada fácilmente por actores malintencionados.

Además del icono del candado, también es importante prestar atención al protocolo utilizado por el sitio web. Los sitios web seguros utilizan el protocolo HTTPS en lugar de HTTP. La "S" adicional significa "seguro" y indica que la conexión está encriptada y autenticada, lo que proporciona una capa adicional de seguridad.

Si no ves el icono del candado, la S al final del http o si el sitio web muestra advertencias de seguridad, es mejor evitar compartir información sensible en ese sitio y buscar alternativas más seguras.

BUSCA COMUNICACIONES POR CANALES ENCRYPTADOS Y DE CONFIANZA

Busca y utiliza plataformas o servicios de correo electrónico y chat que tengan canales **encriptados** de comunicación y que aseguren esa comunicación encriptada de extremo a extremo. Esta tecnología funciona codificando los mensajes, de modo que sólo la remitente y la destinataria puedan descifrarlos. Algunos servicios como Telegram o Whatsapp ofrecen encriptaciones extremo a extremo, lo que los hace fuerte ante terceros atacantes sin embargo no son fuentes que respeten la privacidad, pues venden datos y tiene acuerdos con el estado. Es decir, **nos cuida del ladrón, pero no del opresor ni del policía** y es importante tomarlo en cuenta sobretodo quienes son comunicadoras en defensa del territorio.

Mi amigo: No, WhatsApp no nos espía, son puros inventos y mentiras.



Mientras tanto los de WhatsApp



Signal



CHAT Y MENSAJERÍA INSTÁNTANEA

Aunque muchas aplicaciones usan la encriptación de mensajes de extremo a extremo, Signal ofrece más privacidad en los metadatos y no comparte su información con terceros. Dado que Signal tiene propietarios privados y sin ánimo de lucro, muy probablemente seguirá siendo la opción más segura en el futuro cercano

Existen otras opciones para mensajería instantánea que van más allá en la seguridad, pero requieren un poco más de conocimientos, en ellas podemos dejar de lado los servidores de empresas privadas para nuestra comunicación y usar los nuestros, por ejemplo usando <https://matrix.org/>. O incluso podemos tener una comunicación sin ningún intermediario, utilizando la tecnología del peer to peer (Sí igual que los torrents). Visita <https://briarproject.org/> para más información sobre esta aplicación diseñada para comunicaciones seguras para activistas y personas bajo riesgo.

Para tu servicio de correo seguro existen muchas opciones que puedes considerar. Es crucial que revises detenidamente las características de cada una y elijas aquellas que se ajusten mejor a tus necesidades. La seguridad es un aspecto fundamental a tener en cuenta.



SERVICIO DE CORREO SEGURO Y ENCRIPTADO

Una de las recomendaciones que te podemos hacer es utilizar **riseup.net**. Esta plataforma ofrece un servicio de correo seguro y privado, con encriptación de extremo a extremo y políticas estrictas de privacidad. Además, cuenta con una comunidad activa que se preocupa por la seguridad y la privacidad en línea.



Otra opción a considerar es **Protonmail**. Este proveedor de correo electrónico también se destaca por su enfoque en la seguridad y la privacidad. Utiliza encriptación de extremo a extremo y almacena los correos electrónicos en servidores ubicados en Suiza, conocida por sus estrictas leyes de privacidad.

Si prefieres tener un mayor control sobre tu servicio de correo seguro, también puedes optar por utilizar servidores autónomos de confianza. Aquí una lista con algunas alojados en latinoamérica y otras partes del mundo:

Un **listado de servicios libres** para que los medios comunitarios y organizaciones sociales usen alternativas abiertas y éticas, seguras y respetuosas de la privacidad, autónomas e independientes.

<https://liberaturadio.org/recursos-y-plataformas-libres/>



NO USAR LA MISMA CUENTA PARA INGRESAR A DIFERENTES SERVICIOS

Ahora es común encontrar servicios en línea que te dan la opción de iniciar sesión con tu cuenta de Google. Sin embargo, es crucial comprender los riesgos de utilizar el mismo usuario de Google en otras plataformas. Si una de estas plataformas o servicios sufre una brecha de seguridad o una filtración de datos, la cuenta de Google y de todas las otras plataformas donde hayas iniciado sesión se verá comprometida, lo que puede tener graves consecuencias para la privacidad y seguridad de nosotras.

Iniciar sesión

¿No tienes una cuenta? [Regístrate](#)



Muchas plataformas ofrecen ingresar con tu datos de Google,
esa no es una buena idea

Imagina que tienes una llave maestra que abre todas las puertas de tu casa. Si alguien roba esa llave, tendría acceso a todas las habitaciones y podrían hacer mucho daño. Si usas la cuenta Google en otras plataformas estás dejando esa llave maestra en muchos lados, incrementando considerablemente la posibilidad de ser descubierta y utilizada con malas intenciones.

Para mitigar estos riesgos, es recomendable utilizar identificadores de usuario únicos y contraseñas sólidas para cada plataforma y servicio en línea. De esta manera, si una plataforma se ve comprometida, solo esa cuenta específica se verá afectada, y el resto de las cuentas permanecerán seguras.

AJUSTAR LAS CONFIGURACIONES DE PRIVACIDAD EN REDES SOCIALES

Es muy importante revisar cómo tenemos configurada la privacidad en nuestras redes sociales para evitar que cualquier desconocida pueda ver nuestras publicaciones. En la mayoría de las plataformas podemos configurar si nuestras publicaciones son visibles para toda la red, o sólo para quienes tenemos como contactos o amiga, incluso hay más opciones. A través de estas ellas podemos controlar quién puede ve nuestras fotos, comentarios, estados y toda esa info personal que compartimos. Tener conciencia de las opciones de configuración de privacidad en redes sociales es clave para cuidar nuestra intimidad y mantenernos seguras en línea.

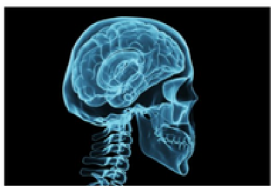
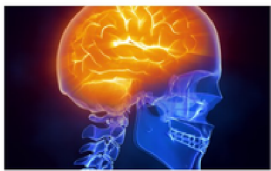


fíjate en las configuraciones de privacidad al publicar en línea y escoge sabiamente

El tema del acoso en Internet es una cosa seria. Si dejamos nuestra cuenta accesible a todo el mundo, podemos atraer atención no deseada y convertirnos en blanco de comentarios malintencionados o bullying en línea. Si compartimos demasiada info personal en modo público, podemos ser víctimas de robo de identidad. Las delincuentes pueden usar esa info para hacerse pasar por nosotras y causarnos problemas financieros y legales. ¡Mejor tener cuidado y mantener esa info privada solo para nuestras amigas y familiares de confianza.

AUTENTICACIÓN MULTIFACTOR

Los servicios digitales han tenido que echar mano de mecanismos que refuercen la seguridad de sus accesos, **uno de los métodos actualmente recomendable es la Autenticación de Doble Factor (MFA o Multi Factor Authentication en inglés)**, que es decirle a la plataforma o servicio dos veces que eres tú a través de vías distintas. Hay varios servicios que ya incluyen la doble autenticación como gmail o facebook, también puedes descargar aplicaciones para autenticar con doble factor usando otro dispositivo, como tu teléfono móvil.

	Poniendo una contraseña fácil para no olvidarla
	Poniendo números y caracteres especiales en mi contraseña
	Activando el doble factor de autenticación

A veces, cuando intentas iniciar sesión en tu cuenta de una plataforma de redes sociales, te encuentras con un proceso de verificación de identidad de dos pasos. Además de ingresar tu nombre de usuario y contraseña, se te solicitará un segundo método de autenticación con otro dispositivo, por lo general tu teléfono celular a través de un mensaje o llamado. Este segundo paso de verificación es importante para garantizar la seguridad de tu cuenta y proteger tus datos personales.

Cuando hasta el atún te pide doble autenticación



Estas son medidas que se han desarrollado para evitar el phishing (concepto que veremos más adelante). En los servicios que podamos usar este método de acceso es recomendable ante el robo de identidad. Las compras digitales son cada día más comunes, por lo tanto, si una plataforma donde compras o vendes te ofrece esta opción, te recomendamos encarecidamente que la utilices.

ACTUALIZA TUS EQUIPOS Y APLICACIONES

Como explicamos anteriormente, el software o programas de computadoras son escritos por seres humanos y, como tal, a veces pueden contener errores en su construcción que no son detectados hasta que el programa ya está disponible al público. Además, con el avance de la tecnología, se descubren nuevas vulnerabilidades que antes no eran conocidas. Estas vulnerabilidades pueden poner en riesgo la seguridad de las usuarias.

Para solucionar estos problemas y reducir los riesgos para las usuarias, existen las actualizaciones. Las actualizaciones son modificaciones que se realizan en el código del software para corregir las vulnerabilidades descubiertas. Estas actualizaciones permiten fortalecer la seguridad del programa y garantizar un mejor funcionamiento.

Es importante destacar que las actualizaciones no solo se enfocan en corregir errores y vulnerabilidades, sino que también pueden incluir nuevas características y mejoras en el rendimiento del software. Esto significa que, al mantener tu software actualizado, no solo estarás protegiendo tu sistema contra posibles amenazas, sino que también podrás disfrutar de nuevas funcionalidades

Los programas “crackeados” si bien son “gratis” estos pierden la capacidad de actualizarse y seguramente estarán llenos de malware. **Los softwares y repositorios no oficiales son lugares peligrosos y es fácil que puedas ser víctima de apps maliciosas.**



UTILIZA HERRAMIENTAS PARA REDUCIR TU HUELLA O RASTRO DIGITAL

Cada vez que interactuamos en línea, desde hacer compras hasta publicar en redes sociales o buscar información, dejamos rastros de datos. Si esta información cae en manos equivocadas, nuestra privacidad puede verse comprometida. Los datos personales pueden ser utilizados para identificar, rastrear o dirigir publicidad no deseada hacia nosotras. Es nuestra huella digital, también conocida como "rastreo digital" o "huella en línea", y se refiere a la información personal que dejamos atrás mientras navegamos por Internet. Esta huella puede ser más grande de lo que pensamos y puede tener varios riesgos asociados.

Es crucial entender que cada clic y cada comentario en línea contribuyen a nuestra reputación digital. Los empleadores, instituciones del estado, amigas y familiares pueden buscar información sobre nosotras en Internet, formando una imagen de quiénes somos basada en nuestras actividades.

Debemos reducir la información que compartimos en línea sin pensar. Antes de hacer clic en "publicar" o proporcionar datos personales en línea, consideremos las posibles repercusiones y cómo esa información podría ser utilizada en el futuro. Al ser conscientes de nuestra huella digital y tomar medidas para controlarla, podemos proteger nuestra privacidad, seguridad y reputación en línea. Para ello les compartimos algunas herramientas.



VPN: Una Red Privada Virtual o VPN toma las comunicaciones que salen de tu computadora o dispositivo hacia su destino final y las envía a través un servidor intermedio. Este servidor intermedio puede estar ubicado en cualquier parte del mundo, lo que hace que parezca que tu conexión proviene de esa ubicación en lugar de tu ubicación física real, haciéndole creer a cualquier sitio web o servicio en línea que estás en otro lugar, ¡incluso en otro país!

Entonces, cuando estás usando una VPN, digamos que estás en casa en Ecuador, pero la VPN hace que parezca que estás en India. Los sitios web y servicios en línea pensarán que estás en India, no en Ecuador. Esto puede ser útil si quieres acceder a contenido que solo está disponible en ciertos países o si simplemente quieres mantener tu ubicación en línea en secreto. Es como navegar por internet desde una ubicación diferente, ¡sin que nadie sepa dónde estás realmente!

En la actualidad, existen numerosos servicios de VPN disponibles en el mercado. Sin embargo, es crucial optar por aquellos que sean de confianza o incluso considerar la posibilidad de configurar y utilizar una VPN propia. Algunos navegadores ofrecen la opción de VPN integrada como una característica adicional. Aunque puede resultar conveniente, es esencial investigar y asegurarse de que estas opciones sean igualmente confiables y respeten tu privacidad.

VPN: Descripción Gráfica



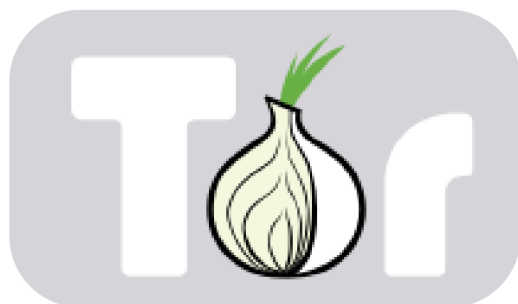
ORBOT: VPN LIBRE Y GRATUITO PARA CELULARES

Orbot te permite escoger específicamente que apps quieres que funcionen de manera segura a través de la red VPN TOR. Esta función es muy útil para personalizar tu navegación privada. <https://orbot.app/es/>



TOR: El Proyecto TOR, también conocido como TOR (The Onion Router), es una red anónima diseñada para proteger la privacidad y la libertad en Internet. Funciona redirigiendo el tráfico de Internet a través de una red distribuida de servidores voluntarios en todo el mundo, en lugar de conectar directamente la usuaria al destino.

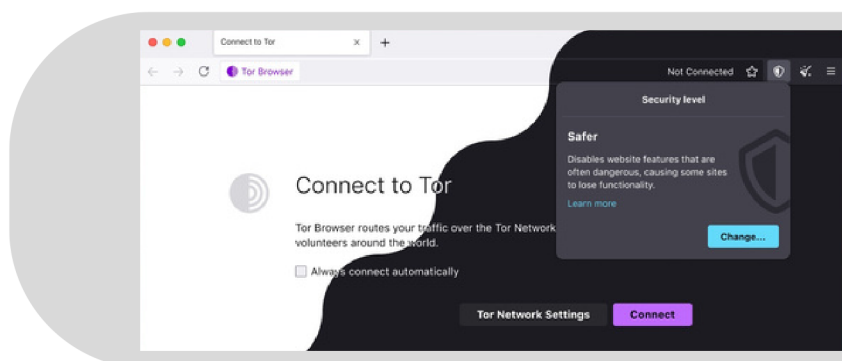
Esta red de retransmisión hace que sea mucho más difícil para cualquier persona, incluidos gobiernos, proveedores de servicios de Internet u otros, rastrear las actividades en línea de la usuaria, su ubicación o identidad.



<https://www.torproject.org>

El nombre "onion router" (Enrutado cebolla en inglés) proviene del enfoque de capas de cebolla utilizado para ocultar la información. Cuando se utiliza TOR, el tráfico de Internet se cifra y se redirige a través de múltiples servidores (nodos) en la red TOR. Cada nodo solo puede ver la dirección IP del nodo anterior y el siguiente en la cadena, lo que dificulta enormemente el rastreo del origen o destino final del tráfico. En otras palabras TOR es una gran red de servidores VPN voluntarios que enmascaran la identidad y la ubicación de las usuarias.

TOR es utilizado por una variedad de personas para una variedad de propósitos, desde proteger la privacidad y la seguridad en línea hasta eludir la censura y el bloqueo de Internet. Sin embargo, también puede ser utilizado para actividades ilegales, por lo que es importante usar TOR de manera ética y responsable.



TOR BROWSER: es un navegador web que utiliza la red Tor para proporcionar anonimato y privacidad en línea, permitiéndonos navegar por la web de forma segura y sin ser rastreadas.

Sin embargo, es importante tener en cuenta que el uso del Tor Browser no garantiza el anonimato completo ni la total seguridad en línea. Además debemos seguir prácticas de seguridad digital adicionales, como evitar la revelación de información personal y mantener nuestros sistemas actualizados.

Aquí hay algunas características clave del Tor Browser:

1. **Navegación Anónima:** Tor Browser utiliza la red Tor para enmascarar nuestra dirección IP, lo que dificulta que los sitios web y terceros rastreen la actividad en línea.
2. **Cifrado de extremo a extremo:** Todas las comunicaciones a través del Tor Browser están encriptadas desde la fuente hasta el destino final, lo que garantiza la privacidad y la seguridad de los datos.
3. **Evadir la censura:** Puede ayudar a eludir la censura en línea al proporcionar acceso a sitios web bloqueados por gobiernos u otros organismos de control.
4. **Protección contra el seguimiento:** Al bloquear los rastreadores y cookies de terceros por defecto, Tor Browser protege la privacidad al limitar la información que los sitios web pueden recopilar sobre nosotras.
5. **Plug-ins de seguridad:** El navegador incluye algunas características de seguridad integradas, como NoScript y HTTPS Everywhere, que ayudan a protegernos contra ataques maliciosos y garantizan una conexión segura a los sitios web.

DESCARGA TOR BROWSER Y PROTÉGETE DEL RASTREO Y LA CENSURA GRACIAS AL APOYO MÚTUO

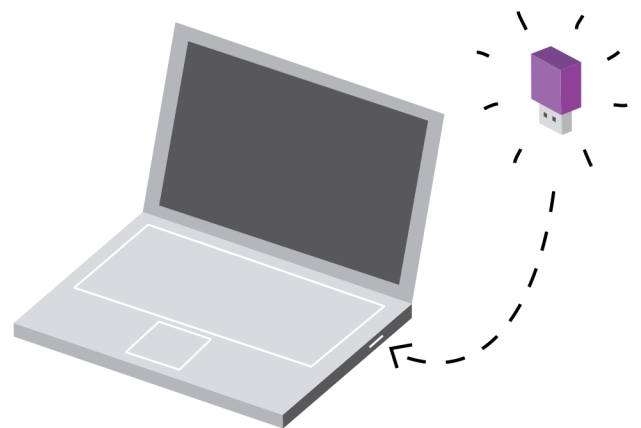
TOR Project, las desarrolladoras de Tor Browser son una organización sin ánimo de lucro y dependen en colaboradoras en todo el mundo para mantener un sistema seguro para millones de personas.





TAILS: Es un sistema operativo portátil que puedes guardar en una memoria USB y ejecutar directamente todos tus programas y archivos desde allí, independiente de la computadora física donde lo hagas. Es como tener una computadora personal completa en tu bolsillo escondida en una USB.

Cuando conectas la memoria USB con TAILS a una computadora cualquiera y la inicias desde ahí, puedes acceder a tu sesión con todas las funciones de una computadora normal, revisar archivos, navegar por Internet, enviar correos electrónicos, editar documentos y más, pero sin modificar nada en la computadora donde pusiste la memoria portátil.



Cuando apagas tu computadora y quitas la memoria USB, desaparece cualquier información que hayas usado o dejado en la sesión y la computadora vuelve a su estado original. Es como si nunca hubieras usado esa computadora.

Esto es muy útil para personas activistas y defensoras de derechos humanos que corren riesgo de que su computadora personal desaparezca o sea destruida. Tails es muy fácil de instalar y usar, incluso si tienes poca experiencia con computadoras.



<https://tails.net/>

El trabajo de TAILS está financiado por donaciones de personas como tú y organizaciones que apoyan la libertad de Internet: Mozilla, Tor, DuckDuckGo, Freedom of the Press Foundation, AccessNow, etc.

<https://www.parrotsec.org/>

Parrot OS es un proyecto de código abierto, lo que significa que es desarrollado y mantenido por una comunidad de voluntarios y desarrolladores de todo el mundo.



PARROT OS: Es un sistema operativo diseñado específicamente para proporcionar herramientas y características avanzadas de seguridad informática y privacidad en línea. Incluye por defecto el navegador anónimo Tor y soporte para VPN junto con herramientas de cifrado de datos para proteger la privacidad.

A pesar de ser una distribución de Linux poderosa y rica en características, Parrot OS está optimizado para ser ligero y rápido, lo que significa que puede ejecutarse eficientemente en una amplia gama de hardware, incluso en sistemas más antiguos o con recursos limitados.



<https://www.kali.org/>

Kali Linux, tiene una comunidad vibrante y activa. Hay foros activos, canales IRC, un sistema abierto de seguimiento de errores e incluso sugerencias de herramientas proporcionadas por la comunidad.

KALI: Kali Linux es una distribución de Linux especializada en pruebas de penetración y auditorías de seguridad. Es una herramienta poderosa utilizada por profesionales de la seguridad informática, investigadoras de vulnerabilidades y hackers éticos para evaluar la seguridad de sistemas informáticos y redes. Fue fundada y es mantenida por Offensive Security Ltd.

Este sistema operativo viene preinstalado con una amplia gama de herramientas de prueba de penetración que permiten a las usuarias identificar y explotar vulnerabilidades en sistemas informáticos y redes. Esto incluye herramientas para el escaneo de puertos, la inyección de SQL, la explotación de vulnerabilidades de software, entre otros.

**BUENAS PRÁCTICAS Y CUIDADOS DIGITALES
PARA TELÉFONOS CELULARES**

MANTÉN TU TELÉFONO BLOQUEADO

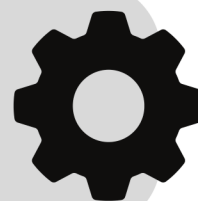
Imagina que te roban el dispositivo o se te pierde y no tiene bloqueo de pantalla. A veces por desconocimiento o simplemente por comodidad, descuidamos la importancia de utilizar esta función. Puede parecer trivial, pero en realidad es una medida crucial para proteger nuestra información personal y privacidad en caso de pérdida o robo del dispositivo. Sin un bloqueo activado, la ladrona o cualquier persona que encuentre nuestro teléfono tendría acceso directo a todos nuestros datos, desde contactos y mensajes hasta aplicaciones bancarias y correos electrónicos. Es como dejar nuestra casa sin cerradura, exponiendo todo lo que tenemos dentro a posibles intrusos.

Para evitar ponernos en riesgo, es esencial tomar medidas proactivas para asegurar nuestro teléfono móvil. Una forma efectiva de hacerlo es estableciendo un bloqueo en la pantalla, que puede ser una contraseña numérica, un código alfanumérico, un patrón de desbloqueo, o incluso la biometría, como la huella dactilar o el reconocimiento facial. Estas opciones de seguridad adicionales ofrecen una capa adicional de protección y dificultan el acceso no autorizado a nuestro dispositivo.

También es muy recomendable conocer a fondo las opciones de seguridad que ofrece nuestro dispositivo móvil y aprovecharlas al máximo. Esto incluye activar funciones como el cifrado de datos, la autenticación de dos factores y la ubicación remota del dispositivo en caso de pérdida o robo. Además, es bueno guardar los datos de compra y el número IMEI (International Mobile Equipment Identity), que es el número de identificación único de cada teléfono (por lo general viene en la tarjeta del chip). Este número te facilita la denuncia y recuperación del dispositivo en caso de pérdida o robo. Con estos pasos simples pero efectivos, podemos proteger nuestra información personal y disfrutar de una experiencia más segura y tranquila.

VE A CONFIGURACIONES

Busca el símbolo de engranes en tu celular para acceder a las configuraciones. Desplázate hacia abajo y busca la sección de "Seguridad" o "Bloqueo de pantalla". El nombre exacto puede variar ligeramente según la versión de sistema operativo que estés utilizando.

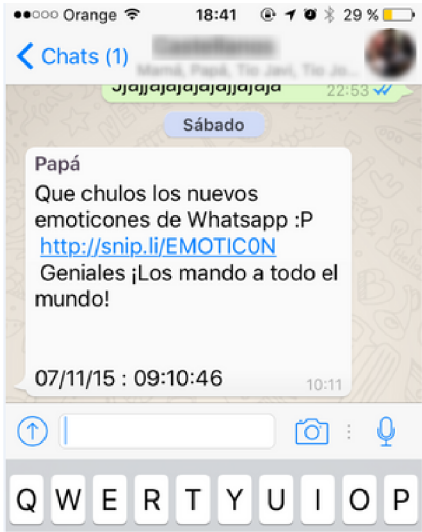


CUIDA LO QUE ENVÍAS Y RECIBES POR MENSAJES DE TEXTO

Los mensajes de texto son una forma común de comunicación, pero también pueden ser un objetivo fácil para ser espiados o leídos por desconocidos. Por esta razón, es esencial que seamos conscientes de los riesgos asociados y evitemos enviar datos confidenciales, como detalles de tarjetas de crédito o información personal importante, a través de mensajes de texto. El envío de este tipo de información puede exponernos a posibles interceptaciones por parte de agentes maliciosos o software espía que puede comprometer nuestra seguridad.

Además, es importante tener precaución con los mensajes de texto que recibimos, ya que algunos podrían contener enlaces o archivos adjuntos maliciosos diseñados para infectar nuestro dispositivo móvil con malware. Estos mensajes suelen utilizar tácticas de **ingeniería social** para engañarnos y hacernos hacer clic en enlaces o archivos peligrosos.

La ingeniería social a través de mensajes de texto también puede involucrar la suplantación de identidad, donde los estafadores se hacen pasar por amigos, familiares o contactos de confianza de la víctima para solicitar información confidencial o realizar solicitudes fraudulentas.



Es importante aprender a reconocer la ingeniería social en los ataques

Para protegerse contra este tipo de ataques es importante ser escépticas ante mensajes no solicitados o inesperados, especialmente si solicitan información confidencial o acciones inusuales. También es recomendable verificar la autenticidad de las remitentes y evitar hacer clic en enlaces o descargar archivos adjuntos de mensajes sospechosos.

VERIFICA ARCHIVOS Y ENLACES DUDOSOS

Imagina que estás en internet navegando y de repente recibes un correo electrónico con un archivo adjunto. Podría ser algo genial, como una foto divertida, ¿verdad? Pero, ¿qué pasa si ese archivo no es lo que parece? Podría ser un virus que dañe tu computadora o robe tu información.

Aquí es donde entra en juego el motor de antivirus. Un motor de antivirus es como una biblioteca que tiene acceso a una gran base de datos de información sobre malware, que son los programas maliciosos. Esta base de datos contiene detalles sobre diferentes tipos de virus, gusanos, troyanos y otros tipos de malware que podrían dañar tu computadora o robar tu información.

El motor de antivirus escanea rápidamente la liga o archivo que le entregues y lo compara con lo que sabe sobre el malware. Si encuentra una coincidencia, te alerta de que el archivo o enlace puede ser peligroso. Esta base de datos se actualiza constantemente porque expertas en seguridad informática están siempre buscando nuevas amenazas



[HTTPS://VIRUSTOTAL.COM](https://virustotal.com)

VirusTotal es una plataforma en línea que permite analizar archivos y URLs en busca de malware utilizando una amplia variedad de motores antivirus y herramientas de escaneo.

Además de utilizar páginas como VirusTotal para verificar enlaces y archivos dudosos, es importante comprender cómo funciona esta herramienta y cuándo es apropiado utilizarla.

Hay que tener en cuenta que, aunque VirusTotal es una herramienta útil, no es infalible. Algunos tipos de malware pueden evadir la detección de los motores antivirus tradicionales, lo que significa que es posible que los motores de antivirus no detecten todas las amenazas potenciales, sobre todo las más recientes.

ACTUALIZA TU SISTEMA OPERATIVO PARA ESTAR PROTEGIDA A NUEVAS AMENAZAS

Las actualizaciones del sistema operativo del teléfono móvil están diseñadas para mejorar tu experiencia en general. Es fundamental mantener tu sistema operativo actualizado para garantizar que tu dispositivo esté protegido contra las últimas amenazas de seguridad y que funcione de manera eficiente.



Buscar seguridad en tu teléfono móvil no se trata solo de instalar contraseñas seguras o configurar ajustes de privacidad, sino también de mantener tu sistema operativo actualizado. Las actualizaciones del sistema operativo suelen incluir parches de seguridad que corrigen nuevas vulnerabilidades conocidas y protegen tu dispositivo contra posibles ataques cibernéticos. Al instalar estas actualizaciones de manera regular, puedes garantizar que tu dispositivo esté protegido contra las últimas amenazas de seguridad descubiertas.

Cómo actualizar el sistema operativo de tu teléfono móvil:

1. Verifica la disponibilidad de actualizaciones: Abre la configuración de tu teléfono móvil y navega hasta la sección de "Actualizaciones del sistema" o "Acerca del dispositivo". Allí, busca la opción que te permita verificar si hay actualizaciones disponibles para tu sistema operativo.

2. Descarga e instala la actualización: Si hay una actualización disponible, sigue las instrucciones en pantalla para descargar e instalar la actualización en tu dispositivo. Para una actualización segura y sin problemas, te aconsejamos que te conectes a una red Wi-Fi en lugar de utilizar tus datos móviles. Las actualizaciones de software suelen implicar la descarga de gran cantidad de datos, lo que puede

consumir rápidamente tu plan de datos móviles y resultar en costos adicionales inesperados en tu factura. Con una conexión Wi-Fi estable, podrás descargar los archivos de actualización de manera más rápida y sin preocupaciones por el consumo de datos.

Además, es crucial realizar la actualización mientras tu dispositivo esté conectado a una toma eléctrica. Durante el proceso de actualización, tu dispositivo está realizando cambios importantes en su sistema operativo y requiere una cantidad significativa de energía. Si la batería de tu dispositivo se agota durante la actualización, existe el riesgo de interrumpir el proceso, lo que podría provocar daños en el equipo o incluso dejarlo inutilizable.



Cada teléfono difiere un poco en sus opciones, pero con curiosidad podemos llegar lejos

3. Reinicia tu dispositivo: Una vez que la actualización se haya descargado e instalado correctamente, es posible que se te solicite reiniciar tu dispositivo para aplicar los cambios. Asegúrate de guardar cualquier trabajo o información importante antes de reiniciar tu dispositivo.

4. Verifica la instalación: Después de reiniciar tu dispositivo, verifica que la actualización se haya instalado correctamente. Puedes hacerlo navegando nuevamente a la sección de "Actualizaciones del sistema" o "Acerca del dispositivo" en la configuración de tu teléfono móvil y comprobando si tu sistema operativo está actualizado a la versión más reciente disponible.

Siguiendo estos sencillos pasos, puedes mantener tu teléfono móvil actualizado con las últimas mejoras de seguridad y rendimiento, garantizando así una experiencia más segura y eficiente en tu dispositivo.

REVISA QUE PERMISOS TIENEN TUS APLICACIONES

Los permisos que solicita una aplicación al momento de instalarla es un aspecto importante a considerar. Algunas aplicaciones pueden pedir acceso a información sensible, como la ubicación, contactos o archivos personales. Antes de otorgar estos permisos, es esencial evaluar si son realmente necesarios para el correcto funcionamiento de la aplicación.

Cuando instalas una app, fíjate bien en los permisos que te pide. Algunas pueden querer acceder a tu ubicación, contactos o archivos personales. Antes de darles luz verde, piensa si realmente necesitan esa información para funcionar bien. Recuerda que dar permisos innecesarios puede ser riesgoso para tu privacidad y seguridad. Por ejemplo, ¿por qué una app de linterna necesita tus contactos? Eso es raro, ¿no? Así que tómate un momento para leer la lista de permisos y decidir si estás de acuerdo con lo que piden.

Además, es una buena idea investigar un poco sobre quién hizo la app y si son de fiar en términos de privacidad y seguridad. Revisa las opiniones de otros usuarios para ver si hay problemas con la privacidad o el uso indebido de datos.



DEJA QUE EXODUS ANALICE TUS APPS

Exodus busca rastreadores integrados y los enumera. En cierto modo, los informes Exodus son una forma de saber cuáles son realmente los ingredientes del pastel que estás comiendo.



Existen varias aplicaciones disponibles en Android que pueden mostrar los permisos concedidos a cada aplicación, estas herramientas también nos informan sobre los llamados permisos y rastreadores de aplicaciones ya instaladas o incluso antes de instalarlas. Esto significa que podemos tener conocimiento previo sobre las posibles implicaciones en términos de privacidad y seguridad antes de decidir instalar una nueva aplicación en nuestro dispositivo.

CONÉCTATE A UNA RED WI-FI DE CONFIANZA

Una de las primeras acciones que realizamos al salir de casa es buscar una red Wi-Fi gratuita para ahorrar datos móviles. Sin embargo, es importante ser conscientes de los riesgos asociados con estas redes públicas no seguras. Estas redes, especialmente las abiertas y no protegidas por contraseñas, pueden ser un terreno fértil para ciberdelincuentes que buscan comprometer la seguridad de los dispositivos conectados.

Una de las mejores prácticas es evitar el uso de redes Wi-Fi gratuitas o públicas y **abstenerse siempre** para acceder a datos sensibles o realizar transacciones financieras en ellas, aunque parezcan seguras como la del aeropuerto o el metro, estas redes están expuestas a posibles ataques de intermediarias maliciosas que intentan interceptar y comprometer nuestros datos mientras estamos conectadas.

También existen las "redes Wi-Fi de phishing" o "puntos de acceso falsos", son una táctica común utilizada por las ciberdelincuentes para capturar información confidencial de personas desprevenidas. Estas redes falsas están diseñadas para imitar a una red legítima y suelen tener nombres similares a los de establecimientos públicos, como

cafeterías, aeropuertos o centros comerciales, para engañar y hacer creer que estamos conectándonos a una red segura y confiable, pero en realidad las ciberdelincuentes pueden interceptar y monitorear todo el tráfico de datos que pasa a través de esa red. Esto incluye información sensible como contraseñas, credenciales, números de tarjetas de crédito y otra información personal y financiera.

Cuando usas una red WiFi gratuita.



Cuando te enteras que esa red es insegura y expone tus datos y tu equipo a software malicioso y robo de información.



CIERRA LA SESIÓN DESPUÉS DE USAR TU CUENTA

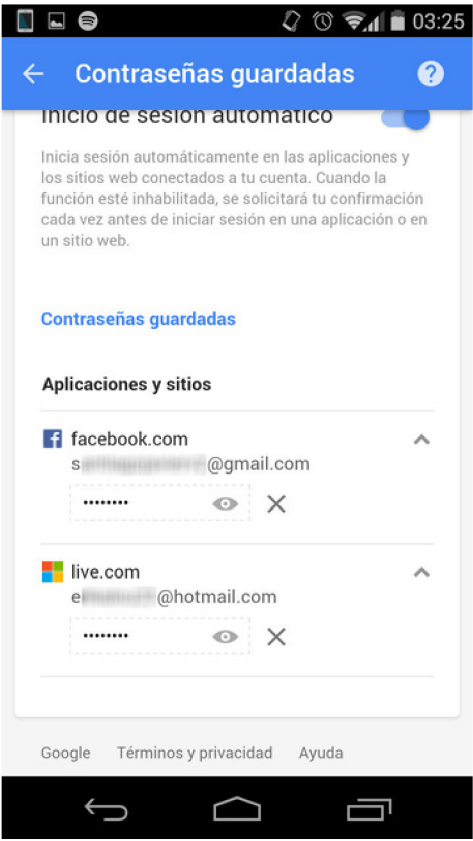
Cuando inicias sesión en una cuenta en línea, como una plataforma de redes sociales, un servicio de correo electrónico o un sitio web de banca en línea, tu sesión queda activa y permaneces conectada a esa cuenta hasta que decides cerrar sesión.

A menudo, cuando ingresamos a nuestras cuentas en línea, simplemente cerramos la ventana del navegador o apagamos nuestro dispositivo móvil sin realizar el proceso de cerrar sesión adecuadamente. Esta práctica común puede llevar a que las cuentas queden abiertas y activas, dejándolas vulnerables a accesos no autorizados o compromisos de seguridad.

Es fundamental cerrar la sesión en los sitios web después de usarla, especialmente al realizar pagos o transacciones bancarias en línea. Al cerrar la sesión, te aseguras de que no quedes conectada de forma permanente, lo que podría exponerte a posibles riesgos de seguridad si alguien más accede a tu dispositivo.

Además, es importante **evitar almacenar tus nombres de usuario y contraseñas** en tu teléfono. Si tu dispositivo móvil se pierde o es robado, cualquier persona que tenga acceso a él también tendría acceso a tus cuentas si las credenciales están almacenadas en el dispositivo. Esto puede poner en peligro la seguridad de tus cuentas y la información personal asociada con ellas.

Dejar que tu teléfono recuerde las contraseñas es una mala práctica



APAGA EL WI-FI Y EL BLUETOOTH CUÁNDO NO LOS USES

Es crucial apagar la función de red wifi y Bluetooth cuando no las estés utilizando activamente en tu dispositivo móvil. Mantener estas funciones activas todo el tiempo puede exponerte a diversos riesgos de seguridad. Por ejemplo, las hackers pueden aprovecharse de esta situación para identificar las redes wifi a las que te has conectado previamente y crear redes falsas que imitan a éstas. Esto se conoce como suplantación de red, donde las atacantes engañan a tu dispositivo para que se conecte a estas redes falsas, lo que les permite interceptar tu tráfico de datos o lanzar ataques cibernéticos.

Cuando te bajas del autobús y tus audifonos bluetooth dejan de sonar.



Además, dejar el Bluetooth encendido constantemente también puede ser peligroso. Las hackers pueden aprovecharse de las vulnerabilidades en la conexión Bluetooth para llevar a cabo ataques de intermediarias. Esto implica que una atacante se interpone entre tu dispositivo y el dispositivo al que estás intentando conectarte a través de Bluetooth, lo que les permite interceptar o modificar la comunicación entre ambos dispositivos. Esta situación puede llevar al robo de información confidencial o al control no autorizado de tus dispositivos.

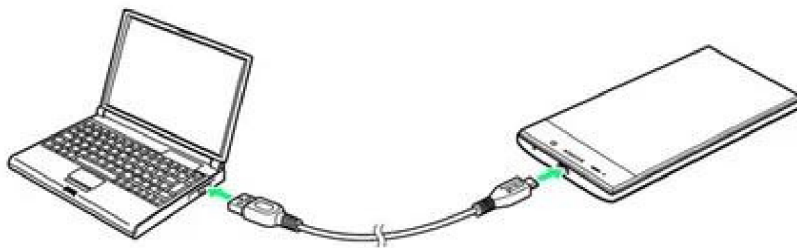
Por lo tanto, es una práctica recomendada apagar la red wifi y el Bluetooth cuando no los necesites activamente. Esto también preservará la vida útil de la batería de tu dispositivo y tampoco despertarás el interés de ciberdelincuentes.

REALIZA COPIAS DE SEGURIDAD REGULARMENTE

Realizar copias de seguridad regularmente es una práctica esencial para proteger tus datos y garantizar la seguridad de tu información personal en dispositivos móviles. A medida que utilizamos nuestros teléfonos para almacenar una gran cantidad de información, desde fotos y videos hasta documentos importantes, la memoria se va llenando hasta agotarse, en ese momento ya no permitirá tomar nuevas fotos y muchas otras funciones se verán afectadas, por ello se recomienda pasar la información del teléfono a otros medios.

Estas copias de seguridad pueden incluir una amplia gama de datos, desde aplicaciones y configuraciones, hasta archivos multimedia y registros de mensajes de chat. Almacenar estos datos de forma segura en un lugar externo, como en una computadora, la nube o en un disco duro externo, proporciona una capa adicional de protección contra la pérdida de datos debido a la falla del dispositivo o a eventos imprevistos como el robo o la pérdida.

Además de realizar copias de seguridad, es importante mantener el dispositivo limpio y organizado. Eliminar regularmente archivos multimedia innecesarios, mensajes de chat antiguos y otros historiales, no solo ayuda a liberar espacio en el dispositivo, sino que también puede contribuir en nuestra privacidad y en disminuir nuestro rastro digital en el teléfono.



Para realizar copias de seguridad, conecta tu teléfono a una computadora y copia las fotos y datos que quieras respaldar. Posteriormente puedes pasar esa información a una nube o un disco duro externo.

REINICIA DE VEZ EN CUANDO TU DISPOSITIVO

Apagar y volver a encender tu dispositivo (reiniciar) de vez en cuando es una práctica simple pero efectiva que puede beneficiar enormemente la salud y la seguridad. Muchas de las infecciones y problemas de rendimiento en los teléfonos móviles pueden estar relacionados con archivos temporales y caché acumulado que actúan como refugio para programas maliciosos. Estos archivos temporales proporcionan un entorno propicio para que los virus y malware se oculten y se repliquen, lo que puede llevar a una infección más profunda y extensa en tu dispositivo.

Al reiniciar el dispositivo de vez en cuando, permites que el sistema se limpie y elimine estos archivos temporales. Al cerrar todas las aplicaciones y procesos en ejecución durante el reinicio, se interrumpen las actividades maliciosas que pueden estar ocurriendo en segundo plano, lo que ayuda a detener la infección en su camino y a evitar daños mayores en tu dispositivo.

Cuando tocas algo en el celular y se te traba

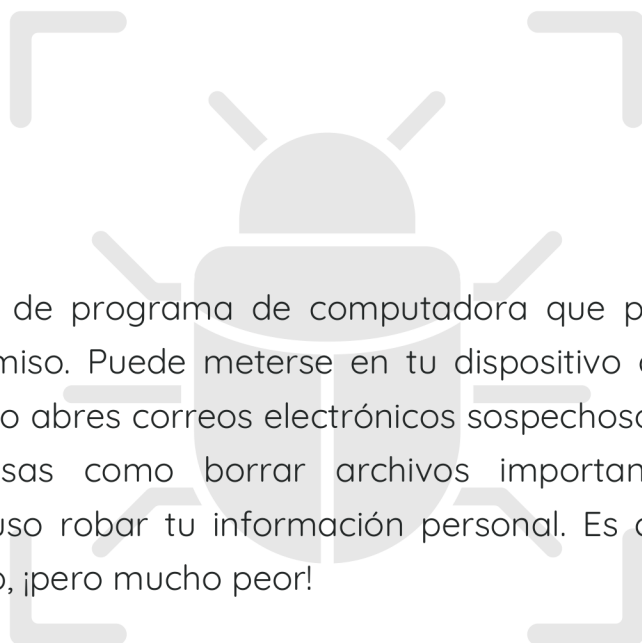


Además de eliminar archivos temporales, reiniciar el dispositivo también puede ser útil para resolver problemas de software que puedan surgir debido a conflictos o errores en el sistema o congelamientos.

Al reinicia tu dispositivo de forma constante, también te aseguras que se instalen actualizaciones de software pendientes. Estas actualizaciones pueden incluir correcciones de errores, mejoras de seguridad y nuevas funciones.

CONOCE LOS DISTINTOS TIPOS DE ATAQUES

A continuación, nos pondremos un poco más técnicas porque revisaremos conceptos relacionados con los diversos tipos de ataques a nivel de software. El ataque más conocido quizás es el virus pero el panorama de amenazas es mucho más amplio y complejo. El término '**malware**', engloba a la gran familia de programas diseñados con intenciones perjudiciales para los sistemas informáticos y la información que contienen. Entre estos programas se incluyen no sólo los virus, sino también troyanos, gusanos, ransomware, spyware y adware, cada uno con sus propias características y métodos de ataque. Es importante comprender la diversidad de estas amenazas para poder implementar medidas efectivas de protección y seguridad informática.



Virus: Es un tipo de programa de computadora que puede hacer cosas malas sin tu permiso. Puede meterse en tu dispositivo cuando descargas cosas de internet o abres correos electrónicos sospechosos. Una vez dentro, puede hacer cosas como borrar archivos importantes, ralentizar tu dispositivo o incluso robar tu información personal. Es como un resfriado para tu dispositivo, ¡pero mucho peor!

Gusanos: A diferencia de un virus, no necesita que hagas nada para infectar tu computadora, como abrir un archivo. Los gusanos son malware que tienen la capacidad de auto replicarse y moverse de una computadora a otra a través de internet. Es como un gusano real que se arrastra por la tierra y puede extenderse rápidamente de un lugar a otro.

Adware: Se trata de un tipo de software que muestra publicidad de manera automática, ya sea mientras se navega por páginas web o durante la instalación de programas. Su objetivo principal es generar ingresos a través de la visualización de anuncios. Aunque algunos adware son inofensivos, otros pueden ser maliciosos y representar una amenaza para la seguridad del dispositivo y la privacidad.

Ransomware: Este software malicioso, derivado del término en inglés 'ransom' (rescate) y 'ware' (software), representa una seria amenaza en el mundo digital. Funciona secuestrando una computadora infectada, impidiendo el acceso a archivos críticos o incluso a todo el sistema. Paralelamente, las ciberdelincuentes dejan un mensaje en la misma computadora donde exigen un rescate económico para restaurar el acceso. Esta forma de extorsión digital puede causar graves daños tanto a nivel personal como empresarial, ya que la pérdida de datos sensibles o el pago del rescate pueden tener repercusiones financieras y de privacidad significativas.

Spyware: Este tipo de software malicioso se infiltra en un dispositivo y opera de manera sigilosa para recopilar información confidencial. Una vez instalado, recoge datos personales y de navegación, como historial de navegación, contraseñas, correos electrónicos y otra información sensible. Posteriormente, transmite estos datos a terceros sin el consentimiento del propietario del dispositivo. Es literalmente un espía en nuestra computadora.

Keylogger: Un keylogger es un tipo de software o dispositivo que registra cada pulsación de teclas realizada en un teclado de computadora o dispositivo móvil. Su objetivo principal es capturar información confidencial como contraseñas, nombres de usuario, mensajes y otros datos de interés. Esta información se almacena en un archivo o se envía a un tercero, sin el conocimiento ni nuestro consentimiento. Los keyloggers pueden ser utilizados de manera legítima para monitorear la actividad en computadoras compartidas o en entornos empresariales, pero también pueden ser implementados de manera maliciosa para robar información personal o comprometer la seguridad de los sistemas.

Troyano: Es un software malicioso diseñado para engañar a las usuarias haciéndoles creer que es un programa legítimo e inofensivo. Como el caballo de Troya, una vez que la usuaria confía y lo ejecuta, el troyano realiza acciones no deseadas dañinas en el dispositivo infectado, como robar información confidencial, obtener acceso no autorizado al sistema o permitir el control remoto del dispositivo por parte de una extraña.

Netbots: Los botnets, también conocidos como redes de bots, son programas informáticos maliciosos que infectan y controlan múltiples dispositivos, como computadoras, teléfonos inteligentes u otros dispositivos conectados a internet. Estos dispositivos infectados son utilizados por el atacante para llevar a cabo diversas acciones sin el conocimiento ni el consentimiento de las propietarias legítimos. Por ejemplo, los botnets pueden ser utilizados para enviar correos electrónicos no deseados (spam), lanzar ataques de denegación de servicio distribuido (DDoS), robar información confidencial, minar criptomonedas u otras actividades maliciosas. Los dispositivos comprometidos en un botnet suelen ser controlados de forma remota por una atacante a través de un servidor centralizado, permitiéndoles coordinar y ejecutar acciones a gran escala.

Zero Click: ES un tipo de software malicioso con la capacidad de infiltrarse en un dispositivo sin requerir ninguna acción por parte de la víctima, como hacer clic en un enlace o descargar un archivo. Estos programas son especialmente peligrosos porque pueden comprometer un dispositivo simplemente estando encendido, sin que nos demos cuenta.

Backdoor: Se refiere a una vulnerabilidad en un programa de computadora que da acceso y control sobre el mismo software. Es cuando por ejemplo un navegador web tiene un falla que permite a una extraña acceder todo nuestro historial y hacer modificaciones a distancia. Estas puertas traseras pueden ser intencionales o resultado de errores en el diseño o la programación del software. Se suelen aprovechar las backdoors para acceder clandestinamente a sistemas y dispositivos.

Rootkit: Imagina que tienes una casa y alguien se esconde dentro sin que te des cuenta. Este "alguien" es como un rootkit en una computadora. Una vez dentro, esta persona puede hacer cosas malas sin que lo notes, como espiar lo que haces o robar cosas. Además, puede esconderse en lugares difíciles de encontrar, como detrás de las paredes o en el sótano, al igual que un rootkit se esconde en partes profundas del sistema de una computadora. Es difícil de detectar y deshacerse de esta persona, al igual que es difícil detectar y eliminar un rootkit de una computadora porque puede esconderse en partes profundas del sistema, como el "root" (raíz), que es la parte más importante de la computadora.

Prueba de penetración (pen test): Es un tipo de simulación de ataque diseñada para identificar posibles vulnerabilidades en sistemas, redes, sitios web, aplicaciones y otros procesos. Mediante este método, se intenta ingresar de manera controlada y ética al sistema como lo haría un atacante real, con el fin de descubrir fallas de seguridad antes de que puedan ser explotadas por ciberdelincuentes.

Ataques de fuerza bruta: son como esos intentos persistentes de adivinar una contraseña, pero realizados por programas informáticos en lugar de personas. Estos softwares prueban millones de combinaciones de contraseñas una tras otra, esperando dar con la correcta y así acceder a una red o servicio en línea sin permiso. Por lo general cuentan con listas enormes de contraseñas posibles y las van probando una tras otra, como un candado con un montón de llaves, ¡pero sin saber cuál es la correcta! Estos ataques pueden tener éxito si la contraseña es fácil de adivinar o está basada en información predecible, pero también pueden llevar mucho tiempo si la contraseña es fuerte y complicada.

Spoofing: Es una técnica utilizada donde se falsifica la información del origen de una comunicación para hacerse pasar por otro sistema o entidad. Esto puede incluir la falsificación de direcciones de correo electrónico, números de teléfono, direcciones IP u otros datos de identificación digitales. El objetivo principal del spoofing es engañar a las destinatarias para que crean que la comunicación o la solicitud proviene de una fuente confiable cuando en realidad no es así.

Ataques de denegación de servicio distribuido (DDoS, por sus siglas en inglés): son una forma de ataque en la que se utiliza una red de computadoras comprometidas, conocidas como "botnets", para inundar una página web o servicio con un gran volumen de tráfico de datos. El objetivo principal de un ataque DDoS es sobrecargar los recursos de la plataforma, como el ancho de banda de red, el procesador o la memoria, lo que hace que el servicio sea inaccesible para las usuarias legítimas. Es como si millones de personas quisieran entrar al mismo tiempo al mismo sitio web, esta cantidad extraordinaria de solicitudes puede hacer colapsar el sistema.

Hay otro tipo de amenazas que forman parte de lo que se conoce como ingeniería social, una táctica que se basa en la premisa de que **el eslabón más débil en las estrategias de ciberseguridad somos los seres humanos**. La ingeniería social se aprovecha de la vulnerabilidad inherente de las personas para detectar y resistir un ataque. En un escenario de ingeniería social, una atacante utiliza la psicología humana para persuadir al objetivo de que realice ciertas acciones, como transferir fondos al atacante, revelar información confidencial o compartir credenciales de acceso. Este enfoque se basa en manipular las emociones humanas, como el miedo, la curiosidad o la confianza, para obtener acceso no autorizado a información sensible o realizar actividades fraudulentas. Conozcamos algunas de las tácticas empleadas.

Phishing: Es la forma más común de ingeniería social, podemos entenderlo como salir de pesca. Los estafadores envían mensajes haciéndose pasar por una persona u organización en la que la víctima confía (por ejemplo, una compañía con la que la víctima tiene negocios) o también envían mensajes con historias sospechosas esperando que alguien caiga, pero en realidad están tratando de engañarte para que les des información personal, como contraseñas, números de tarjeta de crédito o hagas click en un enlace malicioso. El objetivo del phishing es crear una sensación de urgencia, confianza o curiosidad que lleva a la víctima a actuar precipitadamente.

Estos mensajes pueden llegar por correo electrónico, mensajes de texto o incluso llamadas telefónicas, por eso es importante ser muy cuidadoso y verificar siempre la autenticidad del origen de los mensajes antes de compartir cualquier dato personal.

Baiting: Imagina que estás en la web y ves un mensaje o anuncio que dice algo así como "¡Gana un premio increíble!" o "¡Descarga este programa gratis ahora!". Eso podría ser un "cebo" o "anzuelo" para atraerte.

La trampa está en que, cuando haces clic en ese mensaje o descargas ese programa, en lugar de obtener lo prometido, puedes terminar infectando tu dispositivo con programas dañinos o virus. Es como si alguien te ofreciera un regalo envuelto en papel bonito, pero en realidad está lleno de cosas malas.

Tailgating: Es una táctica de ingeniería social en la que personas no autorizadas siguen de cerca a una persona autorizada para ingresar a una zona restringida. Este tipo de ataque aprovecha la confianza y cortesía común en entornos como oficinas, edificios residenciales o instalaciones corporativas.

Imagina que tienes una tarjeta de acceso para entrar a tu oficina y entras por la puerta principal. Sin embargo, alguien que no tiene permiso para ingresar se acerca detrás de ti y se cuela en el edificio justo detrás tuyo, sin usar su propia tarjeta de acceso.

Cebo USB: También conocido como USB Baiting, es un tipo de ataque en el que un software malicioso, o malware, se instala en una memoria USB. El objetivo es que alguien, de manera involuntaria, conecte esa memoria USB infectada a un dispositivo en una red, lo que puede llevar a la infiltración del malware en esa red.

Por ejemplo encuentras una memoria USB abandonada en tu oficina o en un lugar público. Sin sospechar, la conectas a tu computadora para ver qué contiene. Sin embargo, desconoces que la memoria USB está infectada con malware. Al conectarla, el malware se ejecuta automáticamente en tu computadora y puede comprometer la seguridad de tu sistema, permitiendo que los atacantes accedan a tus datos o infecten otros dispositivos en la red.

Este tipo de ataque es especialmente peligroso porque aprovecha la curiosidad natural de las personas y la conveniencia de usar dispositivos USB para transferir archivos.

Spear Phishing: Del inglés spear o lanza, es una forma más sofisticada de ataque de phishing que se dirige específicamente a una persona o grupo en particular. A diferencia del phishing tradicional, que envía correos electrónicos masivos genéricos a una amplia audiencia, el spear phishing utiliza información personalizada y detallada sobre la víctima para aumentar las posibilidades de éxito del ataque. Es como salir de pesca, pero con una lanza.

Las atacantes realizan una investigación exhaustiva sobre la víctima para recopilar información como su nombre, cargo, relaciones laborales, intereses personales y actividades en línea. Luego, utilizan esta información para personalizar los mensajes de phishing de manera que parezcan legítimos y convincentes para la víctima específica.

Los ataques de spear phishing a menudo se utilizan en campañas de ciberespionaje dirigidas a organizaciones gubernamentales, empresas, periodistas o personas defensoras de derechos humanos.

Smishing: Es una forma de ataque de phishing que utiliza mensajes de texto SMS en lugar de correos electrónicos. Estos mensajes de texto fraudulentos suelen parecer provenir de instituciones legítimas, como bancos, empresas de telecomunicaciones o servicios gubernamentales.

Vishing: Tipo de phishing en la que los delincuentes utilizan llamadas telefónicas para engañar a las víctimas y obtener información sensible. Durante la llamada, pueden solicitar información personal o financiera, como números de cuenta bancaria, contraseñas o números de seguridad social, bajo pretextos falsos, como problemas de seguridad o verificaciones de cuentas.



OTROS ATAQUES Y NIVELES DE SEGURIDAD

Además de los ataques comunes como el phishing y el malware, existen otras formas más sofisticadas de ataques que involucran el uso simultáneo de varias herramientas y métodos para acceder a información sensible de la víctima. Estas conjunción de técnicas y herramientas, por lo general están en manos de entidades gubernamentales y actores con importantes recursos financieros, ya que este tipo de ataque involucra una gran cantidad de recursos humanos y técnicos.

Un ejemplo conocido de este tipo de software o servicio espía es Pegasus, desarrollado por una empresa israelí y utilizado por ejércitos y fuerzas policiales en todo el mundo. Pegasus se ha utilizado para seguir a figuras de interés político, periodistas, defensoras de derechos humanos y activistas en varios países. Este software es conocido por su capacidad para infiltrarse en dispositivos de forma sigilosa y sin dejar rastro, y su costo económico es considerablemente alto.

Un informe detallado sobre el uso de Pegasus en México está disponible gracias al trabajo del colectivo r3d. Este informe proporciona una visión en profundidad sobre cómo este software espía ha sido utilizado para llevar a cabo operaciones de vigilancia en el país. Puedes encontrar más información sobre este informe en el siguiente enlace:



INFORME DE R3D SOBRE PEGASUS EN MÉXICO

Pegasus pertenece a la empresa israelí NSO Group. Debido a su licencia de exportación, únicamente puede ser vendido a gobiernos. <https://ejercitoespia.r3d.mx/pegasus/>

Evil twin: es una técnica de suplantación de redes inalámbricas que implica la creación de una red Wi-Fi falsa que imita a una red legítima, por eso su nombre “gemelo malvado” en inglés. Utiliza una antena falsa para interceptar paquetes de datos enviados entre dispositivos y puntos de acceso legítimos. Las usuarias pueden verse atraídos a conectarse a esta red falsa debido a su apariencia similar a la red original.

Una vez que los dispositivos se conectan al Evil Twin, los datos transmitidos entre el dispositivo y la red pueden ser interceptados y manipulados por la atacante. Esto puede permitir acceder a información sensible, como contraseñas, datos bancarios o información personal.

Ataques de hombre en medio del camino. Los ataques Man-in-the-Middle (MitM) implican que una atacante intercepta las comunicaciones de la red para poder espiar o modificar los datos que se transmiten. Aunque este tipo de ataque es posible en diferentes sistemas, los dispositivos móviles son especialmente susceptibles.

Recipient



Carmen Aristegui

Aristegui Noticias

SMS on Dec 24 2015

Carmen 5 days ago that my daughter does not appear, we are desperate, I'll thank you if you help me share her photo: [\[exploit link\]](#)

Translation

Carmen hace 5 días que no aparece mi hija te agradeceré mucho que compartas su foto, estamos desesperados: [\[exploit link\]](#)

Original

SMS on Jun 3 2016

Carmen the website is intermittent, this error appears when you try to get in: [\[exploit link\]](#)

Translation

Carmen la pagina esta intermitente, esta apareciendo este error al intentar ingresar: [\[exploit link\]](#)

Original

RECKLESS EXPLOIT: Mexican Journalists, Lawyers, and a Child Targeted with NSO Spyware

Scott-Railton J, Marczak B, Abdulrazzak B, Crete-Nishihata M & Deibert R

CITIZEN LAB 2017

Caso Pegasus: espiando a la periodista Carmen Aristegui y el método Spear Phishing dónde se ocupó un Baiting para poder infectarla con Malware.

BIBLIOTECA POPULAR DE CULTURA LIBRE

CUIDADOS DIGITALES EN INTERNET

64

CONCLUSIONES

EVALÚA LOS RIESGOS Y CONSTRUYE TUS PROTOCOLOS DE SEGURIDAD

Como te mencionamos antes, no hay una guía mágica que resuelva todos nuestros problemas de seguridad en línea. Por eso, es crucial no solo entender algunas de las herramientas y conceptos que hemos repasado hasta ahora, sino también adoptar un enfoque activo para protegernos en el mundo digital.

Esto implica crear un plan de seguridad digital que se adapte a nuestras necesidades personales y grupales. Ya seas parte de un equipo, una organización, o simplemente una usuaria comprometida, todas podemos mejorar nuestra seguridad en línea.

Podemos comenzar por identificar qué o quiénes queremos proteger. ¿Son nuestros archivos los que necesitan salvaguardarse? ¿O es nuestra computadora y equipo lo que más valoramos? ¿Quizás nuestras comunicaciones son una prioridad? ¿O incluso, lo más importante, nosotras mismas y nuestra privacidad la que queremos proteger?

Una vez que hemos definido qué queremos proteger, el siguiente paso es identificar nuestras prácticas concretas y evaluar el riesgo que representan. Por ejemplo, algunos archivos pueden contener información confidencial o crítica para nuestro trabajo, mientras que otros pueden ser más fácilmente reemplazables. De manera similar, nuestras comunicaciones pueden variar en sensibilidad, desde conversaciones personales hasta datos privados o sensibles.

Esta clasificación nos proporciona una visión clara de dónde debemos enfocar nuestros esfuerzos de protección y qué medidas de seguridad son más urgentes de implementar. Así estamos mejor preparadas para generar ideas y estrategias efectivas que fortalecer nuestra seguridad y privacidad en línea.

Ahora que tenemos un catastro de nuestros “**activos a proteger**” nos toca evaluar nuestra relación con la tecnología en tres niveles. La seguridad de nuestras prácticas diarias respecto a esos “activos”, las herramientas que utilizamos y los agentes que puedan afectar nuestra seguridad.

Como decíamos, La primera capa a evaluar es nuestra relación con la tecnología y el nivel de seguridad de nuestras prácticas diarias. Debemos preguntarnos, por ejemplo: ¿Qué tan seguras son nuestras contraseñas? ¿Tenemos bloqueo en nuestros dispositivos? ¿Está actualizado el Sistema Operativo y las aplicaciones? ¿Tenemos respaldo de nuestras cuentas y archivos? ¿Qué información publicamos en redes sociales y por qué? ¿Descuidamos nuestros teléfonos?.

En un segundo nivel, revisaríamos nuestros servicios de red. ¿A través de qué redes nos conectamos a internet? ¿Qué servicios ocupamos y qué tan seguros son? ¿Hemos revisado sus términos de servicio? ¿Cómo está configurada y quién configura la red en nuestra casa u oficina? ¿Qué tan confiable es el proveedor y su infraestructura de red?.

Un tercer nivel implica considerar el contexto físico y social en el que nos encontramos, evaluando el nivel de riesgo y vulnerabilidad que podríamos enfrentar. ¿En qué contexto político y social nos sentimos vulnerables a ataques a nuestra privacidad? ¿Qué información manejamos y cómo la administramos y resguardamos? ¿Qué información, como datos video o imagen, se utilizan en la organización en la que participamos? ¿Qué agentes maliciosos podrían tener interés en nuestra información?.

Una vez hecho ese análisis a partir del catastro, tenemos nuestra **evaluación de riesgos**. Una evaluación de riesgos es un proceso sistemático para identificar, analizar y evaluar los riesgos potenciales que enfrenta una organización, proyecto o actividad. El objetivo principal de una evaluación de riesgos es entender qué eventos o circunstancias podrían causar daño o pérdida.

Es ahora esencial pensar en formas de mitigación de ataques y en la reparación del daño ante posibles ataques o fallas en el sistema. Si algo sale mal y nuestros datos se ven comprometidos, tenemos un plan. Nos aseguramos de tener copias de seguridad y de notificar a las personas afectadas. También trabajamos con las autoridades para resolver el problema y tomar medidas legales si es necesario.

Estos tres niveles de evaluación no solo nos ayudan a identificar posibles fallas, sino que también nos proporcionan una hoja de ruta para generar respuestas efectivas frente a cualquier amenaza o incidente de seguridad, nuestro **protocolo de seguridad**. El protocolo de seguridad es el resultado de definir el uso de buenas prácticas a partir de nuestras necesidades particulares. Hay varios métodos para las diversas necesidades de seguridad, pero nosotras pensamos que las formas de resolver estos problemas comunes es de manera común.

Hacer una evaluación de riesgos y un protocolo de seguridad es una dinámica colectiva. Al involucrar a todo el grupo en este proceso, podemos obtener una comprensión más completa de los posibles peligros que enfrentamos como colectivo y las medidas necesarias para mitigarlos. Además, esta evaluación y protocolo no sólo se centran en los aspectos técnicos de la seguridad digital, sino que también consideran los aspectos sociales y organizativos que pueden afectar la seguridad de todo el grupo.

La invitación es a encontrar espacios de discusión y acuerdo donde podamos definir, por ejemplo, qué herramientas colectivas de comunicación podemos utilizar para fortalecer nuestra seguridad de forma conjunta. Fortalezcamos nuestra autonomía digital y prepararemos a nuestras comunidades para no ser víctimas de explotación o vigilancia. Al construir un protocolo de seguridad conjunto, estamos empoderando a las personas para que tomen el control de su propia seguridad en línea y no dependan únicamente de las herramientas o sistemas proporcionados por terceros.



me cuidan mis amix, no la policía

Ejercicio práctico: Desarrolla un protocolo de seguridad para el uso de un chat comunitario. Realiza una evaluación de riesgos en los tres niveles propuestos, detallando las distintas vulnerabilidades encontradas. Luego, identifica los puntos débiles en seguridad y propón métodos para abordarlos.

BUSCA Y CONSTRUYE ALTERNATIVAS

En el actual panorama de internet nos enfrentamos a diversos riesgos, pero con cuidados colectivos podemos superarlos. El desarrollo de las Tecnologías de la Información y la Comunicación (TIC) han transformado radicalmente la forma en que nos comunicamos, aprendemos y nos relacionamos en la sociedad moderna. Se han convertido en una poderosa herramienta de difusión y formación política e ideológica, similar a lo que la escuela y la televisión fueron para las sociedades antes de la era digital.

El acceso a la información y la capacidad de comunicarse instantáneamente con personas de todo el mundo son aspectos fundamentales de la vida cotidiana. El internet nos brinda la posibilidad de acceder a una cantidad sin precedentes de conocimiento y recursos, lo que nos permite educarnos, informarnos y expresar nuestras opiniones de manera más amplia y democrática.

Sin embargo, al igual que la televisión y la educación, el internet también puede ser una herramienta de influencia y control. Las plataformas de redes sociales y los sitios web de noticias pueden moldear nuestras percepciones y opiniones políticas, y pueden ser utilizados para difundir desinformación y propaganda. Por lo tanto, es crucial fomentar el pensamiento crítico y la alfabetización mediática para navegar de manera segura y responsable en el mundo digital.

Es crucial crear espacios de debate y capacitación en nuestros círculos familiares, entre amigas y compañeras de nuestras comunidades, donde podamos aprender y buscar soluciones colectivas a las vulnerabilidades de nuestros dispositivos y redes. Al igual que aspiramos a una vida libre de violencia y abuso, también visualizamos y construimos un espacio digital seguro y pensado para el bien común.

El acceso y el beneficio de la tecnología digital y las redes no deberían ser privilegios reservados para algunas, sino que deberían considerarse un bien común y un derecho humano colectivo. Esto significa que todas las personas, independientemente de su origen o situación socioeconómica, deberían tener la oportunidad de acceder a la tecnología y beneficiarse de sus ventajas.

Además, es importante que este acceso se acompañe de medidas que garanticen la privacidad y la seguridad de las personas en línea. Esto implica proteger los datos personales de la vigilancia y el uso no autorizado, así como asegurar que las comunicaciones digitales estén protegidas contra el espionaje y la interferencia indebida.

Las herramientas digitales tienen el poder de unirnos y hacernos más fuertes como comunidad. Trabajemos juntas para crear un internet que sea seguro y acogedor para todas. Capacitarnos y colaborar en proyectos comunitarios son pasos fundamentales para moldear un internet que trascienda las inseguridades impuestas por el capitalismo y nos permita ser más que simples usuarias.

No olvidemos que existe un vasto mundo digital se forja en los pilares de la libertad y la igualdad. La cultura libre está presente el hardware que impulsa nuestros dispositivos hasta el software que potencia nuestras aplicaciones. Existen redes de internet comunitarias que siguen creciendo y conectando a personas de todo el mundo, cada elemento del ecosistema de la sociedad de la información tiene su versión moldeada por estos valores. Es esencial no solo utilizar estas **herramientas libres**, sino también comprender cómo funcionan y cómo pueden influir en nuestras vidas.

Compartir lo que sabemos con otras fortalece nuestras comunidades y hace que nuestras ideas crezcan y se desarrollen. Aunque podemos enfrentar los desafíos solas, es mucho más emocionante hacerlo juntas y construir algo que nos pertenezca a todas.

Algunos de las respuestas y soluciones ya existen y otras se siguen construyendo. La oferta que ofrece el mundo libre es amplia y robusta. Busca alternativas al capitalismo digital. No odies la internet, créala libre.

GLOSARIO

Agente malicioso: Cualquier programa o persona que intenta dañar o comprometer en el contexto de una red de computadoras. Personas que realizan actividades ilegales en línea, como el robo de información personal o la distribución de malware.

Aplicación (App): Es un tipo específico de programa que está diseñado principalmente para ser utilizado por personas en un entorno interactivo, como tu celular.

Archivos: son como cajas digitales que guardan diferentes tipos de información, como videos, documentos de texto o canciones en formato MP3. Algunos archivos se utilizan de manera temporal y luego se eliminan, mientras que otros permanecen con nosotros durante mucho tiempo. Cada archivo tiene su propósito y puede contener datos importantes que queremos conservar o compartir con otras.

Autenticación: Es el proceso mediante el cual se verifica la identidad de una usuaria o dispositivo para asegurar que sean quienes dicen ser. Es una medida de seguridad fundamental en sistemas informáticos y redes para proteger la información y los recursos contra accesos no autorizados.

En términos simples, es cuando nos identificamos (mediante nombre de usuaria y contraseña) para demostrar quienes somos antes de acceder a ciertos lugares o servicios. En el mundo digital, la autenticación puede implicar el uso de contraseñas, códigos PIN, huellas dactilares, tokens de seguridad o métodos biométricos para confirmar la identidad de un usuario o dispositivo.

Auditoría de seguridad: Revisión de los controles, políticas y procedimientos de seguridad de una organización.

Barra de direcciones: La barra de direcciones es una parte fundamental del navegador web, generalmente ubicada en la parte superior de la ventana, donde se muestra la dirección URL o dirección web actual. Es un espacio que podemos seleccionar y escribir en ella la URL o dirección del sitio web al que deseamos acceder.

Cifrado o Encriptación: Es un candado digital que protege la información que enviamos por medios digitales. Funciona convirtiendo nuestros mensajes en un código secreto que solo puede ser entendido por quienes tienen la "llave" correcta para descifrarlo. De esta manera, si alguien intercepta nuestros mensajes, no podrá entender lo que dicen a menos que tenga la llave para descifrar el código. Es como enviar una carta en un sobre sellado: nadie puede leerla a menos que tengan la llave para abrir el sobre.

Correo electrónico: El email funciona de manera similar al correo tradicional, pero en lugar de enviar cartas físicas, las usuarias envían mensajes digitales a través de servidores de correo electrónico. Cada usuaria tiene una dirección de correo electrónico única que se compone de un nombre seguido de un símbolo "@" y el DNS del proveedor de correo electrónico (por ejemplo, nombredeusuario@gmail.com). Los mensajes de correo electrónico pueden contener texto, archivos adjuntos, imágenes y enlaces a sitios web.

"Crack" o programa crackeado: es una forma de usar un programa sin pagar por ello. Es como si alguien encontrara una manera de abrir una puerta cerrada sin tener la llave. Algunas personas alteran el código de un programa para que puedas usarlo sin tener que comprarlo pero muchas veces agregan malware al programa para obtener ganancias ilegales con ello. Además, cuando usas un programa crackeado es muy vulnerable ya que no podrás actualizarlo.

Criptojackin: Malware que se introduce en un dispositivo sin el conocimiento del usuario y utiliza los recursos de ese dispositivo para minar criptomonedas de forma ilegal. En lugar de realizar actividades legítimas de minería de criptomonedas, donde los usuarios voluntariamente dedican sus recursos informáticos, el criptojackin se aprovecha de los recursos de la víctima de manera encubierta y sin su consentimiento.

Ciberbullying: es cuando alguien usa internet o teléfonos móviles para hacer cosas malas a otras personas, como enviar mensajes desagradables, difundir rumores falsos o acosar a alguien en línea. Es como si alguien te estuviera molestando o haciendo daño, pero en internet en lugar de en persona. El ciberbullying puede suceder en redes sociales, mensajes de texto, correos electrónicos o cualquier otra plataforma en línea. Es importante ser amable y respetuoso en línea y denunciar el ciberbullying si lo ves o si te está sucediendo a ti. Todos merecen sentirse seguros y felices en internet.

Ciberseguridad: También conocida como seguridad cibernética, se refiere a todas las medidas y prácticas que se toman para proteger la información digital y los sistemas tecnológicos contra amenazas y ataques maliciosos. Su objetivo principal es garantizar la confidencialidad, integridad y disponibilidad de la información.

Cryptomonedas: Son una forma de dinero digital que utiliza la criptografía para asegurar y verificar transacciones, así como para controlar la creación de nuevas unidades de esa moneda. En lugar de depender de un banco central o una autoridad gubernamental, las criptomonedas funcionan en una red descentralizada de computadoras. Bitcoin es la criptomoneda más conocida, pero hay muchas otras, como Ethereum, Ripple y Litecoin.

Datos (Data): También conocidos como información, son cualquier tipo de información que puede ser interpretada, procesada o almacenada por una computadora. Estos pueden ser números, texto, imágenes, sonidos u otros tipos de información que se manipulan en un entorno digital.

Datos biométricos: Se refieren a características físicas únicas que pueden utilizarse para identificar a una persona. Estas características incluyen huellas dactilares, rasgos faciales, patrones del iris y la voz. Los datos biométricos son especialmente útiles en sistemas de seguridad y autenticación, ya que son difíciles de falsificar y proporcionan una forma más segura de verificar la identidad de una persona en comparación con las contraseñas o los pines. Sin embargo, es importante proteger la privacidad de los datos biométricos y asegurarse de que se utilicen de manera ética y legal.

Datos públicos: Los datos públicos son información que ya está disponible para el público en general y generalmente no representan un riesgo significativo si son vistos o compartidos por otras personas. Esta información puede incluir datos que se encuentran en registros públicos, como listas de directorios, registros de propiedad, registros comerciales y datos gubernamentales abiertos. También puede abarcar información que una persona haya optado por hacer pública, como perfiles en redes sociales, publicaciones en blogs o sitios web personales.

Datos privados: Información sensible que está destinada a ser confidencial y no debe ser divulgada al público en general. Estos datos pueden incluir detalles personales como nombres completos, direcciones, números de teléfono, direcciones de correo electrónico, números de seguro social, números de identificación personal, información financiera, registros médicos y cualquier otra información sensible que pueda identificar o afectar la privacidad de un individuo.

Día cero: El concepto de "día cero" se refiere a un tipo específico de ataque cibernético que se produce aprovechando una vulnerabilidad previamente desconocida en un sistema o software. Esto significa que los hackers utilizan esta vulnerabilidad antes de que el fabricante o desarrollador del sistema tenga conocimiento de la falla, dejando a los usuarios vulnerables a ataques sin tener la posibilidad de tomar medidas preventivas.

Dirección IP: Es como la "placa" de identificación de un dispositivo en internet. Imagina que cada dispositivo conectado a internet tiene su propia "placa" con un número único, y esa placa es la dirección IP. Esta dirección permite que los dispositivos se comuniquen entre sí y sepan dónde enviar y recibir información. Por ejemplo, cuando visitas una página web, tu dispositivo envía una solicitud a esa dirección IP para ver el contenido de la página. Es como si estuvieras enviando una carta a una dirección específica para recibir información de vuelta.

Una dirección IP cuenta con 4 segmentos separados por un punto. Cada segmento va del número 1 al 255. Los siguientes son ejemplos de números IP válidos:

192.168.1.254

200.30.40.10

76.23.45.78

Diccionarios de ataque: Son bases de datos que las ciberdelincuentes utilizan en los ataques de fuerza bruta. Gigantescos listados de contraseñas comunes o contraseñas que han sido previamente comprometidas en brechas de seguridad. Las atacantes utilizan estos diccionarios para intentar acceder a sistemas o cuentas al probar automáticamente una gran cantidad de combinaciones de usuario y contraseña. Estos ataques pueden ser muy efectivos contra cuentas que tienen contraseñas débiles o comunes.

DNS: Sistema de Nombres de Dominio (Domain Name System en inglés), es como el "directorio telefónico" de Internet. Cada computadora en internet tiene un número IP asignado el cuál se utiliza para lograr la conexión. Para el ser humano es muy difícil recordar números para cada servicio en internet. Para ello existe el DNS, que traduce los nombres de dominio (por ejemplo wikipedia.com) en su dirección de IP correspondiente (por ejemplo 192.0.2.1). Esto es invisible para las usuarias, ya que sucede de manera automatizada.

Enlace malicioso: Vínculo que parece llevar a un sitio web legítimo o confiable, pero en realidad te redirige a un sitio web malicioso o instala malware en tu dispositivo. Estos enlaces suelen estar ocultos en correos electrónicos, mensajes de texto o en sitios web falsos.

Hacktivista: Es alguien que utiliza sus habilidades con el propósito de promover un cambio social o político en el contexto de las redes informáticas. A menudo, los hacktivistas buscan destacar problemas de injusticia social, corrupción gubernamental o violaciones de derechos

humanos. Sus acciones pueden incluir la divulgación de información confidencial o la interrupción de servicios en línea como una forma de protesta.

Hacker: Describe a alguien que utiliza sus habilidades en computadoras para varios propósitos. Un "hacker ético" es alguien que usa sus habilidades para mejorar la seguridad de sistemas informáticos, identificando y corrigiendo vulnerabilidades antes de que puedan ser explotadas por otros. Por otro lado, un "hacker no ético" o "malintencionado" es aquel que busca comprometer la seguridad de sistemas o redes informáticas con fines delictivos, como robar datos personales o realizar actividades ilegales.

Hardware: Son todas las partes físicas y tangibles de una computadora o dispositivo electrónico. Esto incluye componentes como la unidad central de procesamiento (CPU), la memoria RAM, el disco duro, la placa madre, el teclado, el ratón, la pantalla y otros dispositivos periféricos. En resumen, el hardware es todo lo que puedes tocar y ver en un dispositivo electrónico.

Ingeniería social: Técnica de manipulación que busca engañar a las personas para obtener información confidencial o persuadirlas a realizar ciertas acciones.

Malware: Es un término general que engloba una amplia variedad de programas (software) diseñados con intenciones dañinas.

Mensajes de texto SMS: Abreviatura de Short Message Service, son pequeños mensajes de texto que se envían entre teléfonos móviles por la red de telefonía. Estos mensajes permiten a las usuarias comunicarse de manera rápida y directa, generalmente limitados a un máximo de 160 caracteres. Los SMS han sido una forma popular de comunicación durante muchos años debido a su simplicidad y accesibilidad, aunque en la actualidad han sido en gran parte reemplazados por aplicaciones de mensajería instantánea que permiten enviar mensajes más largos y multimedia.

Metadato: Los metadatos son datos que proporcionan información sobre otros datos. En otras palabras, son datos que describen y proporcionan información adicional sobre un archivo digital. Por ejemplo, en un archivo de imagen, los metadatos pueden contener información sobre la ubicación geográfica donde se tomó la foto, la cámara utilizada, la fecha y la hora, entre otros detalles que podrían comprometer la privacidad si se comparten inadvertidamente.

Navegador Web: Un navegador web es un programa que utilizamos para "navegar en internet". Permite ver la información que contiene una página web. El navegador interpreta el código en el que está escrita la página web y lo presenta en la pantalla permitiendo al usuario interactuar con su contenido. Ejemplos: Google Chrome, Firefox, Tor Browser, Microsoft Edge, Brave.

La "Nube": Conjunto de computadoras ubicadas en centros de datos remotos que almacenan recursos y datos. Estos recursos y datos pueden ser accedidos a través de Internet desde cualquier lugar y en cualquier momento. La nube permite a los usuarios almacenar, gestionar y procesar información sin necesidad de depender exclusivamente de la capacidad de almacenamiento o procesamiento de sus computadoras o celulares

Peer to peer (P2P): significa de persona a persona. Es una forma de compartir cosas directamente entre computadoras, sin necesidad de un servidor central. Imagina que tienes un libro genial y quieres prestarlo a tu amigo. En lugar de pasar por un intermediario, como un servicio de envío o paquetería, simplemente se lo das directamente a tu amigo.

Así es como funciona el P2P en internet: las computadoras se conectan directamente entre sí para compartir archivos, música, videos y más, sin depender de un servidor central. Es una forma rápida y eficiente de intercambiar cosas entre las personas en línea..

Plataforma o servicio web: Una plataforma o servicio web es un conjunto de recursos y herramientas alojados en servidores que permiten a las usuarias acceder a diversas funciones, aplicaciones o servicios. Estos servicios son accesibles a través de un navegador web y a menudo se utilizan para realizar tareas específicas o colaborativas en línea. Algunos ejemplos comunes de

plataformas o servicios web incluyen redes sociales como Facebook, Twitter y LinkedIn, servicios de almacenamiento en la nube como Google Drive y Dropbox, plataformas de streaming de video como YouTube y Netflix, y aplicaciones de productividad como Google Workspace y Nextcloud.

Protocolo de Seguridad: Un protocolo de seguridad es como un plan de emergencia digital. Consiste en una serie de procedimientos y reglas establecidas para responder rápidamente a cualquier amenaza o brecha de seguridad que pueda surgir. Es como tener un manual de instrucciones listo para actuar en caso de que algo salga mal en el mundo cibernético.

Servidor: Los servidores son piezas clave en nuestro día a día en internet. Son las computadoras que almacenan y gestionan todo tipo de información, desde nuestros correos electrónicos hasta nuestras publicaciones en redes sociales. Incluso, cuando accedemos a la nube para guardar nuestros archivos, estamos utilizando servidores. De hecho, cada vez que visitamos una página web, estamos accediendo a la información que estos servidores almacenan y gestionan.

Estas computadoras especializadas, los servidores, están distribuidas por todo el mundo y están conectadas a internet. Su función principal es almacenar, procesar y entregar información a los usuarios que la soliciten. Sin ellos, no podríamos enviar un correo electrónico, subir una foto a nuestras redes sociales o incluso ver un video en línea. Los servidores son la infraestructura invisible pero fundamental que sustenta el funcionamiento de internet.

Sistema operativo: Es el software principal que administra y controla todas las operaciones básicas de una computadora o dispositivo electrónico. Actúa como intermediario entre el hardware (componentes físicos) y el software de la computadora, permitiendo que los programas se comuniquen con el hardware y realicen tareas específicas. El sistema operativo es como el director de una orquesta, coordinando todas las partes de la computadora para que funcionen juntas de manera eficiente y permitiendo que los usuarios interactúen con la máquina de manera fácil y efectiva.

Software: El software es el conjunto de programas, archivos y datos que utilizamos en una computadora o dispositivo electrónico. Incluye los programas y aplicaciones que nos permiten navegar por internet, enviar mensajes, editar fotos o reproducir música. Los archivos de video, texto, música también son software. Y abarca incluso los sistemas operativos, que son como el corazón de la computadora y controlan cómo funciona todo.

Software libre: El software libre promueve la colaboración, la transparencia y el acceso abierto al código fuente de los programas que utilizamos, lo que permite a las usuarias comprender cómo funciona el software y contribuir a su mejora continua. Un ejemplo de software libre es el sistema operativo Linux y muchas de sus aplicaciones asociadas.

Spam: Es todo ese montón de publicidad no deseada en tu buzón de correo electrónico o en tu celular. Son esos correos o mensajes que no has pedido y que llenan tu bandeja de entrada con cosas que no te interesan. A veces, el spam puede contener anuncios molestos, pero otras veces puede ser peligroso.

Torrent: un torrent es una forma de compartir archivos por internet. Piensa en él como un montón de gente compartiendo partes de un archivo en lugar de un solo lugar que tiene todo el archivo. Cuando descargas algo usando un torrent, tu computadora toma pequeñas partes del archivo de muchas otras computadoras que ya lo tienen. Después de que tu computadora tenga todas esas partes, las pone juntas para formar el archivo completo. Es como si estuvieras construyendo un rompecabezas usando piezas de diferentes personas. Los torrents son populares para compartir grandes archivos, como películas, música o programas de computadora, de manera rápida y eficiente.

URL o dirección web: Es una secuencia de caracteres que identifica la ubicación de un recurso en internet. Básicamente, es la dirección que utilizamos para acceder a páginas web, archivos, imágenes u otros recursos en la web. Por ejemplo, una URL es "https://www.ejemplo.com/pagina"

VPN (Red privada virtual): Una VPN es como una capa extra de seguridad para tu conexión a internet. Lo que hace es cambiar tu dirección IP pública y ocultar tu ubicación real para que tu navegación sea más segura y privada. Es como si pusieras una máscara en tu identidad en línea para que los sitios web no puedan rastrear tus movimientos tan fácilmente.

Vulnerabilidad: Una vulnerabilidad es una debilidad en un sistema, aplicación o red que puede ser explotada por una amenaza para causar daño o comprometer la seguridad. Estas debilidades pueden ser fruto de errores de programación, configuraciones incorrectas, falta de actualizaciones de seguridad, diseño defectuoso (software) o por resultado de acciones humanas (ingeniería social).

Violación de la seguridad: Ocurre cuando alguien obtiene acceso no autorizado a sistemas, aplicaciones, redes o dispositivos. Esto puede suceder debido a una serie de razones, como contraseñas débiles, falta de actualizaciones de seguridad, errores humanos o explotación de vulnerabilidades en el software. Cuando se produce una violación de la seguridad, puede resultar en el robo de información confidencial, la interrupción de servicios o el acceso no autorizado a recursos importantes.

LIGAS DE INTERES

Correo

- Riseup <https://riseup.net>
- Protonmail <https://proton.me/>

Blog

- Noblogs <https://noblogs.org>
- Suttty <https://suttty.nl>

Redes Sociales

- Mastodont <https://joinmastodon.org/es>
- Diaspora <https://diasp.org/>

Ofimática

- Open Office <https://www.openoffice.org/>
- Libre Office <https://es.libreoffice.org/>
- Pad Yanapak <https://pad.yanapak.org>
- Calc Yanapak <https://calc.yanapak.org>

Navegadores

- Tor <https://www.torproject.org/es/>
- Chromium <https://www.chromium.org/>
- Brave <https://brave.com/>
- Firefox <https://www.mozilla.org/es-MX/firefox/>

Repositorio de apps Android

- F Droid <https://f-droid.org/es/>

Chat

- Signal <https://signal.org/es/>
- Matrix <https://matrix.org/>

VPN:

- Bitmask <https://bitmask.net/es>

Manifiesto por la Guerrilla del Acceso Abierto

https://colectivodisonancia.net/wp-content/uploads/2020/12/Swartz_manifiesto_Online.pdf

Autodefensa Digital para activistas y comunicadorxs populares

https://utopia.partidopirata.com.ar/zines/autodefensa_digital_para_activistes.html

Politizar la Tecnología: Radios comunitarios y derecho a la comunicación en entornos digitales.

<https://radioslibres.net/politizar-la-tecnologia/>

Tecnologías de vigilancia: tipos de herramientas y sus alcances

<https://protege.la/tecnologias-de-vigilancia-tipos-de-herramientas-y-sus-alcances/>

Escuela de Seguridad Digital (Colnodo)

<https://escueladeseguridaddigital.co/>

Guía: Seguridad digital para las personas defensoras de la Tierra

<https://www.earthdefenderstoolkit.com/kit-de-herramientas/seguridad-digital-para-las-personas-defensoras/?lang=es>

Red en Defensa de los Derechos Digitales (R3D)

<https://r3d.mx/>

Aplicaciones Libres y de Código abierto para Android

<https://fossdroid.com/>

Guardian Project

<https://guardianproject.info/>

Compilado de Guías Prácticas de Seguridad Digital (por Cacú)

<https://share.mayfirst.org/s/ixeyi5rNYMAtzfj>

S.O.S Periodista: Kit de seguridad digital para periodistas

<https://www.tedic.org/s-o-s-periodista-kit-de-seguridad-digital-para-periodistas/>





**NO ODIAS A LOS MEDIOS,
SIÉMBRALOS LIBRES**

Ante la creciente centralización, privatización y uso no consentido de nuestra data personal en internet, creemos fundamental comenzar a cuestionarnos la propiedad de las plataformas e infraestructuras que actualmente sostienen nuestras comunicaciones digitales. Para ello ponemos a disposición este tercer cuadernillo de la Biblioteca Popular de Cultura Libre, dónde se compilan en un lenguaje sencillo conocimientos sobre cuidados digitales.



con el apoyo de:

Cultural Survival



CITSAC

Centro de Investigación en Tecnologías
y Saberes Comunitarios



**CEFO
INDIGENA**

CENTRO DE FORTALECIMIENTO DE LOS
DERECHOS DE LOS PUEBLOS INDIGENAS