#OPNEWBLOOD

LA GUÍA DEL NEWFAG*

AS SEEN ON TV

*LA MÁS MEJOR Y GENIAL Y ÚNICA MARAVILLOSA GUÍA PARA PRINCIPIANTES

Índice

Introducción

Bienvenido a esta nueva edición de la ya archiconocidísima guía para principiantes de Anonymous.

#OpNewBlood no es más que una operación para todos aquellos que estén interesados en ser partícipes de Anonymous y se sientan como unos completos newfags (o lo que es lo mismo, que no tengan ni idea sobre este mundillo).

Esta guía resume brevemente qué es Anonymous, dónde nació y qué objetivos tiene, además de ayudar y dar consejos sobre cómo actuar en la Red y cómo protegerse del Gran Hermano siempre acechante, de los espías que monotorizan cada uno de nuestros movimientos. No existe ninguna versión fija, única u oficial de esta guía, pues Anonymous, como todas las cosas en este mundo, está en constante cambio. El mundo que habitamos se reinventa con cada una de vuestras aportaciones… Bienvenidos a la era del software libre.

¿Qué es Anonymous?

Es difícil responder a esta pregunta. Lo que no es Anonymous es un grupo de hackers antisociales que comen patatas de bolsa en los sótanos de sus casas mientras ojean porno. Básicamente porque no tenemos sótanos, lo demás quizás sea cierto pero no es un requisito indispensable: si tú ojeas el porno con un vermut eres igualmente bienvenido.

Anonymous nació en 4chan, concretamente en el innombrable y a la vez más renombrado canal /b/. Su historia es una de esas grandes historias que cualquier niño ansía escuchar antes de sumirse en sueños, la historia de unos caballeros valientes e irreverentes que por no temer, no han temido ni las normas socialmente más aceptadas y establecidas. Su historia la encontraréis brevemente reseñada al final, con tal de que podamos pasar directamente a la esencia y conozcáis desde un primer momento los valiosos consejos que han de acompañarnos en esta, vuestra mágica y legendaria gran aventura a través del mundo cibernético.

Las grandes filtraciones realizadas por Anonymous no han sido siempre fruto de una incursión informática. Muchas veces, como en el caso de Chelsea Manning, Edward Snowden, o como ha sucedido con las cuentas del Partido Popular este pasado verano de 2013, han sido personas

concretas que, teniendo en sus manos una información privilegiada que consideraron que tenía que ser de dominio público, decidieron publicarla. Todos nosotros tenemos acceso a parte de esa información: se encuentra en nuestros puestos de trabajo, centros educativos, bibliotecas, etc. Está sola y desamparada, llorando porque no vamos en su busca y la mostramos ante los ojos del mundo entero. La información es coqueta y quiere lucirse, y como Anonymous, estás casado con ella. Todos sus caprichos forman parte de tu deber como buen samaritano.

Anonymous infecta mentes, y lo hace cuestionándose todo lo que otros tienen como establecido y natural. El caos nos acompaña, es parte de nuestra fuerza, y su función es dejar patas arriba todo el sistema tal y como lo hemos conocido hasta ahora. Ellos no lo saben, pero el mundo del mañana nos pertenece. La infección sigue contagiándose, y ahora ha llegado a ti: sabes que el mundo no es lo que te han enseñado y estás ante un dilema moral. Estás infectado. Es cuestión de tiempo: pronto empezarás a hacerte preguntas y pervertirás a todos los que te rodean. Nos estamos haciendo con el control del mundo. Bienvenido al País de las Maravillas.

Las colmenas

En anteriores ediciones de OpNewBlood se facilitaba el acceso a un servidor de IRC llamado AnonOps, pero eso se acabó. AnonOps (también conocido como AnonUPS!) fue el escenario de las detenciones de 2011 (aquel rollo de la cópula y la cúpula, y el ridículo supino de la policía nacional cogiendo una máscara de Guy Fawkes como muestra inculpatoria en una rueda de prensa en la que hablaban sobre un caso del que demostraron no tener ni puta idea).

Algunos listillos creyeron que con cambiar de servidor todo quedaba solucionado, y se pasaron a AnonNet dando lugar a las segundas detenciones. Después de estos pequeños fallos saldados con la libertad de varios compañeros tenemos moraleja: IRC = CACA (como diría Carlos, el becario de @policia). Ese medio sólo sirve para el ASL, y lo último que queremos es doxearnos*.

Anonymous no es una sala de chat pública con la BIT (Brigada de Investigación Tecnológica) como invitada VIP. Anonymous somos todos. Anonymous es un concepto, una Idea que defiende el Conocimiento Libre. Y cualquiera que le haga un favor a esta señorita se convierte en su protegido.

En Anonymous abundan los lobos solitarios. Somos el antihéroe del siglo XXI, donde la simiesca cara sonriente de Obama se aparece en todas las pantallas de nuestras computadoras vigilando cada uno de nuestros movimientos, empeñados en tener una vida privada. Pero sabemos que somos legión, y que unidos como uno y divididos por cero no tenemos rival. Por eso hemos generado

millones de colmenas individuales, conectadas a su vez entre sí.

La mejor manera de trabajar es formando una de estas colmenas con personas de suma confianza, y coordinarse con el resto de colmenas para ser un Todo. Por supuesto, no hace falta decir que NUNCA hay que revelar información personal a NADIE. JAMÁS.

colmena.

1. f. Lugar o recipiente donde viven las abejas y fabrican los panales de miel.
2. Conjunto de abejas alojadas en él.

La colmena es el lugar donde las abejas hacen sus panales, formados por un grupo de celdillas de cera que utilizan para depositar la miel. En cada celda vive una sola abeja, pero trabaja conjuntamente con el resto del ejambre para fabricar la miel.

La miel es una fabulosa metáfora para referirse al Conocimiento y Michel de Montaigne ya la utilizó en su día haciendo un paralelismo entre los alumnos y las abejas, quienes recogen el polen de su maestro para luego, posteriormente, sacar su propia miel. Con esto quería remarcar la importancia de tomar el Conocimiento de allí donde se aparezca, pero siempre para acabar alcanzando cada uno sus propias conclusiones.

En Anonymous se hace un poco de todo esto. Por una parte, amamos el Conocimiento y nos postramos ante él para ofrecerle nuestros servicios y liberarlo de allí donde se encuentre prisionero. Nunca damos nada por sentado y siempre continuamos haciéndonos preguntas para que cada persona, ejerciendo su Libertad, se forme su propia Idea del mundo. No queremos que haya un control sobre el Pensamiento. Por otro lado, y para conseguir todo esto, actuamos en forma de colmenas: somos individuos que, en sus propias celdillas (ordenadores), trabajan en conjunto con un grupo de personas para obtener Conocimiento. No nos conocemos, esa no es la finalidad de nuestras acciones, y trabajamos en colmenas porque es la única manera en la que se puede establecer un grupo de confianza. En Internet no puedes confiar en cualquiera, de hecho no debes confiar en nadie, y cuanto más general sea un canal de trabajo más fácil será que se cuele un infiltrado. Por eso trabajamos de este modo. Luego, independientemente, una colmena puede ponerse en contacto con otra para establecer un plan estratégico y desarrollar alguna operación, pero el trabajo delicado siempre se desarrollará entre pequeños grupos preestablecidos y de confianza.

En ningún caso estamos diciendo que esto tenga que ser así, sencillamente funciona así. Y la razón de que sea hoy este el funcionamiento de Anonymous se debe al devenir de los acontecimientos. En un futuro próximo, quizás, la estrategia se habrá modificado de forma espontánea.

*Quedarnos en pelotas. Básicamente, que se averigüe toda tu información personal y sea filtrada a través de Internet con la consecuencia de una posible y segura detención.

La seguridad

Para proteger tu seguridad debes tener en cuenta que lo más importante es el sentido común. Si te pasas de listo, te las verás no solamente con la policía sino con el propio movimiento que se volverá en tu contra. Esto es Anonymous, y nos importa un pimiento lo maravilloso que puedas creerte. Los egofags y attention whores han sido la principal causa de las detenciones de nuestros hermanos, y no estamos dispuestos a dejar pasar un solo descuido en este aspecto. No uses un mismo nick en dos sitios, ni te dediques a hacerte alguien de renombre; para eso tienes a tu colmena que es el resultado de la conglomeración de diversos perfiles y nunca de uno. Es más fácil detener a una persona trazando su perfil psicológico que a través de un rastreo por el ciberespacio.

Más adelante te ofreceremos algunos programas que te ayudarán a anonimizar tu conexión, otro requisito indispensable en un mundo donde el Gran Hermano que George Orwell describió en su obra "1984" es ya una realidad, pero primero ten en cuenta algunos consejos:

- Tu nombre, la edad que tienes, el lugar donde vives o a qué dedicas, son pistas sobre tu verdadera identidad. No confíes en nadie. A veces atravesarás momentos complicados en estos lares, pero has de ser fuerte para mantener tu integridad y no patinar. La policía está infiltrada y los momentos de euforia o debilidad son los que les permiten conocer mejor a sus objetivos: tu vida personal no le concierne a nadie más que a ti mismo, y eso incluye todos tus gustos.
- A lo largo de la historia de Anonymous hemos salido a las calles en diversas ocasiones ya sea para empapelarlas (paperstorms) o para colapsarlas. En 2011 se llevaron a cabo numerosas operaciones en España fuera de Internet como la famosa OpGoya, pero también otras como OpVdeVotaciones, OpSócrates u OpAcademia. En otros lugares del mundo también se han llevado a cabo distintas operaciones callejeras. Con el paso del tiempo hemos llegado a la conclusión de que es mejor evitar estas acciones, pero de llevarlas a cabo no olvides que aquellos con quienes te des cita pueden ser también policías. No reveles tu nick a NADIE, cualquier nombre que uses en Internet no debe poder relacionarse con tu nombre real. Y ve con cuidado, se tiene conocimiento sobre unas listas ilegales que la policía está llevando a cabo a partir de identificaciones en manifestaciones, y cuando la

manifestación es de Anonymous SIEMPRE se encargan de identificar a todo el mundo.

- Tu forma de escribir te delata. La mejor manera de evitar esto es escribir con corrección: si usas ciertos diminutivos como “q”, “k” o “ke” en lugar de “que”, “tmpc” en lugar de “tampoco”, etc., o pones tildes donde no van y puntos después de los signos de exclamación o interrogación, estás dando pistas. Una persona que te sigue en Twitter puede identificarte en un comunicado o en alguna sala de chat. Tus expresiones y smileys también dicen mucho acerca de la persona que escribe. Debes tener siempre presentes todos estos factores.
- Las redes sociales son el lugar en el que estás más expuesto. Si tienes en cuenta todos los consejos anteriores tendrás un mundo ganado, pero quedan otros muchos factores: tus amigos y/o seguidores son uno de los más peligrosos. Cualquier persona con un mínimo de inteligencia investigará las primeras cuentas a las que empezaste a seguir en Twitter y, lo que es más importante, las primeras cuentas que te empezaron a seguir a ti. Naturalmente, las personas a las que más menciones también irán completando tu perfil psicológico. Ten mucho cuidado con esto.
- A la hora de hablar de redes sociales es fundamental recordarte que Facebook trabaja mano a mano con el gobierno de Estados Unidos, y este es aliado de la mayor parte de países del mundo. Ni se te ocurra meterte allí para soltar información delicada, ni siquiera por privado. En cuanto a Twitter, por mucho que tú borres los DM (Direct Messages o mensajes directos) estos no se borran del servidor. Si la policía acaba pidiendo datos sobre tu cuenta, podría acceder a todos ellos. Lo mejor es que nunca trates información de máxima seguridad en ninguno de estos lugares y los dediques al cibersexo. Siempre va bien tener entretenida a la policía.
- TODOS los archivos contienen metadatos: no la cagues por un descuido como subir una fotografía de las tetas de tu novia realizada por tu cámara o teléfono móvil sin haberlos borrado previamente. Lo mejor que puedes hacer para subir una fotografía o un pequeño texto es realizar una impresión de pantalla y pegarla en un estúpido programa como Paint. Luego la guardas, y lista para surbir.

Para preservar el anonimato en Internet, es necesario conocer algunos programas o herramientas que te permiten anonimizar tus conexiones, pero ten en cuenta que la seguridad al 100% es inviable, por lo tanto recuerda utilizar el sentido común.

A continuación, se detallan algunas de las principales huellas o rastros que se dejan en la Red, es importante aprender cómo funcionan las conexiones en Internet comunmente:

- **Email:** Lo que haces al escribir un mail es conectar con tu servidor de correo para acceder a la opción de "redactar". Una vez lo envías, es tu servidor el que se lo pasa a otro servidor, encargado de pasárselo a tu destinatario. Esto no pasa solamente con los e-mails, pasa también con los chats con pasarela.
- **Chat o Web:** En el caso del chat hablas con gente de un mismo servidor: por gTalk sólo hablas con gente en gtalk, por Skype sólo hablas con gente en Skype, etc. En cuanto a chats vía web, sólo está el servidor web, y en el caso de que sea un foro donde hablan varias personas, más de lo mismo: todos conectan a dicho servidor web y no otro, y en él dejan sus mensajes.

Con todo esto lo que queremos decir es que al hablar con otra persona ya sea por e-mail, chat o a través de un foro, podemos dejar nuestro rastro y lo dejaremos, pues todos los servidores guardan logs. También podemos dejar huellas en el ordenador que estemos usando. Hay que tener cuidado con esto. En este segundo caso, es recomendable usar IMAP para gestionar el correo, que no guardar logs, y limpiar siempre el caché antes de cerrar el navegador.

Por último esta el **ISP**, nuestro proveedor de Internet (que suele ser el mismo proveedor de nuestra línea de teléfono). Toda conexión a Internet la realizamos a través de nuestro ISP, quien se encarga de enrutar nuestros paquetes al destino que nosotros deseamos. Por tanto, a través del ISP, se puede conocer todo lo que hacemos en la Red a menos que utilicemos conexiones cifradas, motivo por el que es tan importante el uso de VPN's y proxies, ya que impiden que nuestro ISP actúe como Gran Hermano. Aunque las conexiones se realizan siempre a través del ISP, podemos camuflar nuestro tráfico.

Cuando nos queramos informar sobre la seguridad de cualquier medio que queramos utilizar tenemos que distinguir entre la seguridad a nivel de cliente y la seguridad a nivel de servidor.

A nivel de cliente: En este caso la conexión es segura. Aquí se incluirían sistemas de comunicación cifrados donde los clientes se conectan directamente o se envían e-mails cifrados con PGP -el uso de enigmail sería un ejemplo, pues permite cifrar los correos de forma que tu servidor no los puede ver y siendo sólo accesibles para el destinatario. Existen también este tipo de opciones para algunos chats.

A nivel de servidor: No se puede rastrear el contenido de lo que enviamos entre el servidor y el usuario (sólo la IP del servidor al que se conecta). Un ejemplo es el caso de las conexiones SSL, que cifran todo el tráfico hasta el servidor en donde se descifra y, si ha de reenviarlo, vuelve a hacerlo de forma cifrada. Este paso de descifrado es el punto clave en este nivel de seguridad, pues significa

que el servidor puede guardar nuestras comunicaciones sin cifrar y saber qué es lo que hacemos.

Por tanto, por motivos evidentes, tenemos que buscar siempre que podamos sistemas de comunicación que tengan la seguridad a nivel de cliente asegurada.

Y ahora, pasemos a cosas más concretas. Pero recuerda:

1) No deposites jamás toda tu confianza en ningún software que utilices para tu anonimato.

2) Si vas a hacer algo fuera de la ley y tienes dudas sobre la privacidad que te brinda X herramienta, no la uses.

3) **No hay nada inmaculado y perfecto**. Y si lo hay, sigue la regla 43* (véase: The rules of the Internet).

¡Anonimiza tu navegador!

Lo ideal sería que utilizases un navegador anónimo como **Startpage** que no registra tu dirección IP y cuyos resultados de búsqueda son los mismos que los de Google. Pero si no nos vas a hacer caso en esto, te daremos algunos consejos para el uso de los navegadores más clásicos.

Aunque aún pueda quedar algún que otro detractor, no dudes que tu navegador amigo por excelencia entre los más famosillos es **FIREFOX**. Es en el que sin lugar a dudas podrás navegar de forma más anónima aunque quizás no tan rápido, pero dado el aumento de la censura y la criminalización que estamos sufriendo, es el más recomendable. En Firefox tienes muchísimos addons a tu disposición para controlar tu anonimato e incluso visualizar qué webs siguen tu rastro. Pero, **¡OJO!** Al descargar y utilizar estas extensiones estás confiando en el desarrollador de los mismos, que puede o no ser de fiar. Ya no estamos hablando de la política de privacidad de Firefox sino de cada uno de los desarroladores de los addons en cada caso.

Lo primero que cualquier persona debería hacer es usar una VPN para ocultar su IP, no sólo desde tu ordenador personal sino para cualquier sistema, plataforma o medio a través del cual te vayas a conectar a Internet. Existen VPN's gratuitas y otras de pago y te hablamos de ellas detalladamente más adelante.

Como buscador todos sabemos que Google es el mejor, pero es precisamente porque tiene ojos puestos en todas partes. No le llaman Dios por casualidad: tiene omnipresencia, y es complicado estar a resguardo. Hay otros buscadores alternativos como DuckDuck Go o Bing. Sin embargo, si estas opciones no te convencen, estamos en la obligación de informarte de que dentro de Google tenemos la opción de búsqueda mediante SSL (encriptada), de forma que tus búsquedas quedan

codificadas para quienes traten de controlarlas (algo que a Facebook, por ejemplo, le gusta mucho hacer para luego ponerte anuncios personalizados). La web de esta opción del archifamoso buscador es: https://encrypted.google.com/. Puedes hacerla página de inicio, e incluso añadirla a la barra de buscadores de Firefox, donde también puedes añadir otros buscadores encriptados de portales famosos como YouTube, Wikipedia o Twitter. ¡Y muchos más que habrá y que puedes buscar entre los addons del Firefox poniendo el tag 'SSL'!

Algunos de ellos son imprescindibles, y te los mencionamos a continuación:

Mientras no uses una VPN, o incluso mejor al tiempo que la usas, te recomendamos que añadas en tu navegador Firefox el addon 'anonimoX'. Lo que hace es cambiar tu IP por otra distinta que se te mostrará en la barra de navegación de forma que sabrás en todo momento qué IP estás usando. Además borra todas las cookies de los lugares que visitas, y te permite poner distintas direcciones IP para distintas webs. Tiene muchas opciones de configuración. Lo mejor que podemos decirte es que la pruebes tú mismo.

Collusion no sirve para esconder tu IP si no para saber quién está siguiendo tu pista, quién te está espiando o monitorizando tus pasos en la red. Te muestra las distintas páginas, pero no te da opción de impedirles que te sigan siguiendo. No obstante es útil: el conocimiento siempre es poder.

AdBlock plus: bloquea la publicidad molesta de los sitios webs que visites. Para evitar que te molesten estos banners recomendamos tenerlo siempre activado.

AdBlock plus pop-up: bloquea los pop-up de publicidad, complementa al AdBlock plus.

Better privacy: te ofrece protección especial para las cookies de larga duración. Este addon se hizo para cerciorar a los usuarios sobre esos objetos escondidos, que nunca desaparecen, y para ofrecer un modo más sencillo de gestionarlos desde que los navegadores son incapaces de hacerlo por tí.

Bloody vikings: simplifica el uso de los e-mails temporales ayudándote a proteger tu IP de spam y permaneciendo anónimo. Soporta los siguientes servidores: 10minutemail.com, anonbox.net, mailinator.com, yopmail.com, dispostable.com, mailcatch.com, mailforspam.com, spamavert.com, trash-mail.com, koszmail.pl.

Dt Whois: botón de Domaintools Whois para hacer un whois rápido y sencillo.

Do not Track Plus(esta no ha sido testeada): supuestamente, es un buen complemento al Ghostery. Bloquea más de 600 tracers.

HttpsEverywhere: sirve para cifrar la información enviada o recibida entre el navegador y los sitios web que visites. Fuerza a buscar el protocolo "https" en cada sitio que visites.

NoScript: tú eliges qué JavaScript y plugins permitir (incluso permitirlos temporalmente, si quieres) en cada sitio web que visites y cuáles no.

FoxyProxy: es una herramienta de administración de proxies avanzada. Automatiza el proceso manual de modificar los parámetros de las propiedades de conexión de Firefox. El cambio de servidor proxy depende de la página a cargar y de las reglas de selección definidas por el usuario.

GreaseMonkey: te permite personalizar la manera que un sitio web se muestra o su comportamiento mediante pequeños fragmentos de JavaScript.

Ghostery: bloquea scripts de compañías como Google Analytics, Facebook, etc (ocultos en sitios webs) que tracean tu movimiento por la red.

Todas estas utilidades y recursos que tenemos y tenéis a vuestro alcance para anonimizar vuestro paso por la Red, a parte de ser una precaución necesaria dados los tiempos que corren, constituye un acto de rebeldía en sí mismo en esta era de la "información", centrada en la información privada de todos los ciudadanos.

La tendencia actual, vistas las legislaciones que se quieren implantar por parte de los gobiernos, deja entrever que intentarán que Internet tienda día tras día a una mayor vinculación entre navegación e identidad real, algo que va evidentemente en contra de los propios principios y naturaleza de la Red.

Usemos las herramientas que tenemos a nuestro alcance y reclamemos nuestro derecho a usarlas, no nos limitemos a quejarnos el día que nos las arrebaten.

Servicios de e-mail encriptados.

HushMail Este servicio de email privado localizado en Canadá ofrece cuentas de tipo personal o negocio, incluyendo una certificación extra de tipo HIPAA requerida para organismos como hospitales. Cualquier correo enviado entre usuarios de HushMail es automáticamente cifrado y descifrado, mientras que aquellos mensajes salientes hacia plataformas sin securizar (como Gmail) pueden ser abiertos mediante una contraseña previamente establecida entre ambas partes. A pesar de quedar fuera del alcance del gobierno de Estados Unidos, la empresa propietaria establece en las FAQ que está obligada a cumplir con las leyes canadienses.

S-Mail S-Mail emplea cifrado y SSL para enviar emails seguros hacia otras direcciones del mismo tipo, manteniendo el mensaje y los meta-datos a salvo. Sin embargo, carece de cifrado end-to-end,

con lo cual no se protegerán aquellos mensajes que vayan a parar a otras redes externas. A pesar de no mostrar una dirección física, se ha determinado que el servicio se encuentra en Arizona, por lo tanto ofrece los mismo inconvenientes de permanecer en suelo americano.

O!Polis Encriptado punto a punto de forma gratuita.

Luego, independientemente del navegador que utilices la mejor opción para tu correo electrónico es anonmail. Sin embargo, tiene sus inconvenientes, como que tu cuenta se borra si no inicias sesión en un mes o que tiene muy poco espacio (en la opción gratuita, claro). Por otro lado, puedes encriptar tus correos y no estás bajo el control de Google o Microsoft, quienes cada día hacen más modificaciones de privacidad, mermándola y no haciéndola más fuerte como deberían. Dentro de no mucho tiempo será sin duda obligatorio poner tu número de móvil para activar una nueva cuenta, y seguramente para mantener alguna anterior si la tuvieses también.

VPN

Una **VPN** es una "*Virtual Private Network*", lo que se traduce como una "*Red Privada Virtual*". A través del funcionamiento de una VPN se consigue que los datos que envías y recibes en la Red pasen sobre una red compartida, con lo que tu IP (*número asignado para cada dispositivo que tengas conectado a la red, que permite la identificación de tus dispositivos en Internet*) queda oculta por otra IP asignada por la red que utiliza la VPN.

Podéis encontrar multitud de VPN's, algunas de ellas gratuitas y otras de pago. Desde Anonymous aconsejamos utilizar siempre una VPN de pago puesto que son las más seguras. Las gratuitas suelen guardar los logs de tus movimientos y no dudan dos veces en entregar la información a la policía cuando la solicitan.

Como métodos de pago utilizaremos aquellos que puedan realizarse de manera anónima:

- **Cashu:** Es un sistema de pago mediante tarjetas magnéticas que contienen distintos valores, similares a las tarjetas de prepago utilizadas en telefonía móvil. Podéis encontrar más información y puntos de venta en la siguiente dirección.
    - www.cashu.com
- **Paysafecard:** Los pagos a través de Paysafecard se hacen a través de una tarjeta prepago que puede variar entre los 10€ hasta los 100€. No es necesario indicar datos personales, bancarios ni de tarjeta de crédito.
    - www.paysafecard.com/es-es

- **PerfectMoney:** Es otro sistema de pago mediante tarjeta de prepago. Se pueden encontrar tarjetas entre los 10€ hasta los 1000€.
    - perfectmoney.is/prepaid_cards.html
- **Bitcoin:** El Bitcoin es una moneda digital descentralizada. No está sujeta a controles bancarios ni a gobiernos. Las transacciones que se realizan a través del bitcoin son anónimas, ya que al realizar las compras no es necesario revelar ningún dato sensible sobre tu tarjeta de crédito o cuenta bancaria.
    - www.queesbitcoin.info

A continuación, presentamos una lista de **VPN's** con sus respectivas características.

VPN's que aceptan como método de pago Cashu

- Cactusvpn cactusvpn.com
- Microvpn microvpn.com
- Ivacy ivacy.com

VPN's que aceptan como método de pago Paysafecard

- Ipredator ipredator.se
- TuVpn www.tuvpn.com
- Hideipvpn Hideipvpn.com

VPN's que aceptan como método de pago PerfectMoney

- Ovpn ovpn.to
- DoubleVpn www.doublevpn.com/en
- VpnLab vpnlab.ru

VPN's que aceptan como método de pago Bitcoin

- Airvpn airvpn.org/plans
- PureVpn www.purevpn.com
- VpnLab vpnlab.ru

VPN's gratuitas

- CyberGhost cyberghostvpn.com
- Hotspot Shield www.hotspotshield.com
- OpenVPN www.openvpn.net
- ProXPN proxpn.com
- Spotflux www.spotflux.com

Estas últimas se han añadido como uso de protección adicional en casos no comprometedores: sirven para incomodar nuestro rastreo, ya que si reciben una orden judicial lo más seguro es que den los datos de los usuarios como decíamos.

TOR

Tor es una red abierta que existe *encima* de la Internet que todos conocemos. Aprovecha la infraestructura que las redes proporcionan (desde los cables hasta los protocolos de comunicacion e intercambio de paquetes) para crear una red accesible tan sólo bajo determinadas condiciones. Primero veamos cómo conectarnos a Tor, luego discutiremos las ventajas que eso nos proporciona.

¿Cómo nos conectamos a la red Tor?

- **Manera fácil y aconsejada**: el Tor Browser Bundle (TBB). Es un paquete con todo lo necesario para conectar un navegador web (el *Tor Browser*, basado en Firefox) a la red Tor. Tened en cuenta que **SÓLO** el tráfico que sale del Tor Browser va a usar la red Tor. El resto del tráfico que sale de vuestra máquina no usará Tor. Haced la prueba: conectaos a whatismyipaddress.com para conocer vuestra dirección IP desde el Tor Browser y desde otro navegador, veréis que el resultado es distinto.
- Tor puede usarse para conectar a la red otros programas, no sólo navegadores. Para una instalación y un uso más general de Tor seguid los consejos de @adastra en su blog y leed las primeras entradas de su serie "Preservando el Anonimato y Extendiendo su Uso", empezando aquí Es de contenido altamente técnico, así que si no entendéis lo que leéis, mejor que no lo pongáis en práctica. Aún así, seguro que aprendéis algo, pues las explicaciones de @adastra son excelentes. Por otra parte, si entendéis bien el blog mencionado, ¿qué hacéis leyendo un documento #OpNewBlood? XD

A partir de aquí, supondremos que usáis el TBB.

Es extraordinariamente importante (MUY importante) leer estas advertencias antes de usar Tor. También es muy importante que estéis al día y mantengáis el TBB actualizado con las últimas versiones que aparezcan. Pensad que una de las maneras que la NSA usó para detectar y arrestar usuarios de Tor (no por ser usuarios de Tor, sino por ser pedófilos, bien por la NSA XD) fue aprovechar una vulnerabilidad en el Tor Browser Bundle (de hecho, era una vulnerabilidad de Firefox, ver este artículo para los detalles y aquí encontraréis un resumen fácil de entender).

Algunos detalles

Una vez conectados a la red Tor, el tráfico destinado a Tor (y sólo este) saldrá de nuestro ordenador cifrado, conectándose a un nodo de entrada de la red Tor. Una vez dentro, el tráfico pasará por, como mínimo, otro servidor más de la red Tor hasta llegar a un nodo de salida. De ese nodo de salida el tráfico saldrá tal y como debería haber salido de nuestro ordenador si no hubiéramos estado conectados a Tor. Es decir, si nos conectamos a una web sin cifrado alguno (p.ej. conexiones http) el tráfico saldrá de Tor en plano, sin cifrar, tal como hubiera salido de nuestra máquina sin Tor. Eso sí, con una IP distinta, así que seremos anónimos (a no ser que nos delatemos en el contenido de ese tráfico, p.ej. enviando un formulario con información personal). Sin embargo, si de origen ya establecemos una conexión cifrada (p.ej. usando https), también saldrá cifrada del nodo de salida de Tor. En definitiva, nuestro tráfico sale del nodo de salida de Tor tal como hubiera salido de nuestro ordenador si no hubiéramos estado conectados a Tor.

Además, los servidores dentro de la red Tor sirven para algo más que para dejar pasar tráfico cifrado. Pueden albergar servicios ocultos (hidden services), es decir, aplicaciones web como las que ya conocemos (correo, tiendas, chats, blogs, repositorios, etc.) sólo accesibles dentro de la red Tor. Su url típicamente termina en **.onion** y sólo puede resolverse desde dentro de la red Tor. Estos servicios son ideales para todo tipo de actividad que requiera una dosis muy alta de anonimato, p.ej. el activismo político en España XD

¿Qué conseguimos?

- La IP con la que nuestro tráfico llega a su destino es la IP del nodo de salida de Tor. Nadie sabe quiénes somos.
- En principio es muy difícil el rastreo (¡no es imposible!) gracias a haber pasado por, como mínimo, tres servidores dentro de la red Tor(el circuito: nodo de entrada, nodo de salida y nodo intermedio). Además este circuito va cambiando mientras estamos conectados, escogiendo nodos al azar dentro de la red Tor. Si miramos cual es nuestra IP mientras usamos Tor, veremos que va variando.

- Podemos acceder a servicios ocultos (.onion) en los que conspirar con cierta tranquilidad XD

Si usamos una VPN simultaneamente a Tor el resultado es que el tráfico destinado a Tor sale de la VPN, así que al final obtenemos:
mi pc —> vpn —> tor —> Internet
Para intentar ser anónimos incluso para la vpn, con algo parecido a:
mi pc —> tor —> vpn —> internet
deberíais pedir al proveedor vpn que cambie algunos detalles de la configuración de la vpn, pero es más bien complicado.

Tened en cuenta que NO hay que usar Tor para:

- Ataques DDOS. Si lo hacéis, estaréis atacando Tor en realidad.
- BitTorrent y similares. Tor no es una red pensada para usar en contextos p2p. Para esto una VPN es ideal.

La documentación en el sitio de Tor, torproject.org es muy buena, por si queréis informaros más.

Finalmente, sólo mencionar que hay sistemas operativos que se aseguran que TODO su tráfico sale por Tor como Tails, pero hay ciertas reglas de uso que hay que respetar; ved tails.boum.org. Y también existe Tor para Android: Orbot (guardianproject.info/apps/orbot).

Por último, enlaces a los documentos filtrados por Edward Snowden que hacen referencia a Tor:
www.theguardian.com/world/interactive/2...
www.theguardian.com/world/interactive/2...
www.theguardian.com/world/interactive/2...
apps.washingtonpost.com/g/page/world/ns...
s3.documentcloud.org/documents/801433/d...
s3.documentcloud.org/documents/801434/d...
s3.documentcloud.org/documents/801435/d...

y algunos de los artículos que, con mayor o menor éxito, los explican para que lo entienda todo el mundo:
www.techspot.com/downloads/5183-tor.html
www.techspot.com/news/54244-nsa-has-had...
www.theguardian.com/world/2013/oct/04/n...
www.theguardian.com/world/2013/oct/04/t...

blog.torproject.org/blog/tor-and-silk-r...

Anonymous recomienda **no** utilizarlo como método para sustituir la VPN, debe ser utilizado de manera complementaria a esta, proporcionando un extra de seguridad y anonimato.

Proxies

Un **proxy** es un servidor que actúa de intermediario entre tu PC e Internet, haciendo que tu IP visible no sea la de tu PC, sino la del servidor proxy. El proxy aumenta tu anonimato, pero una vez más aconsejamos utilizarlo junto con una VPN.

Lista de proxies:

- www.xroxy.com

La configuración de un proxy es distinta para cada navegador.

- **Mozilla Firefox**
  - red.agro.uba.ar/redi-firefox
- **Internet Explorer**
  - support.microsoft.com/kb/135982/es
- **Google Chrome**
  - www.ehowenespanol.com/servidor-proxy-go...
- **Opera**
  - http://wiki.hacktivistas.net/index.php?title=Manual_anticensura:_Proxy#Opera
- **Safari**
  - http://wiki.hacktivistas.net/index.php?title=Manual_anticensura:_Proxy#Safari

DNS

El **DNS** se traduce como el **Servidor de Nombre de Dominio** y su finalidad es traducir las URL's en las direcciones IP's que tengan asignadas cada una de las URL's. Cada ISP utiliza unos DNS propios, por tanto, a la hora de navegar, podría revelar nuestra identidad.

Los DNS asignados por nuestros ISP's pueden ser cambiados por unos DNS libres, facilitando de

esta manera nuestro anonimato. A continuación facilitamos una lista de **DNS** libres.

- **German Privacy Foundation**
    - 87.118.100.175
    - 94.75.228.29
- **OpenDNS**
    - 208.67.222.222
    - 208.67.220.220
- **Swiss Privacy Foundation**
    - 62.141.58.13
    - 87.118.104.203
    - 87.118.109.2

I2P

I2P es una red anónima que alberga diversas aplicaciones para correo electrónico, intercambio de ficheros, IRC, mensajería instantanea, entre otras tantas. Todos los datos son cifrados, de manera que atraviesan varios nodos y se mezclan con otros datos pertenecientes a los usuarios que se encuentren dentro de la red **I2P**, es decir, cada uno de los clientes conectados a la red contribuyen a su funcionamiento.

El uso de esta red es gratuita y las aplicaciones son de código abierto. Puede usarse tanto en Windows como en Linux.

- i2p2.de

Más allá del “hack”

Muchas de las personas que estéis leyendo esta guía pensareis que no teneis ningún lugar en anonymous porque no sois “hackers” o teneis un nivel informático adecuado, nada mas lejos de la realidad, anonymous es un colectivo muy complejo y en el caben muchos tipos de activistas, no necesariamente tienen todos que ser “hackers”.

Hay diversas “colmenas” de anonymous y muchas de ellas no se encargan de temas técnicos, sino de la realización de charlas,recursos multimedia,campañas,etc..

A continuación podréis encontrar una lista de herramientas que os ayudaran, a realizar el trabajo que hemos comentado.

Tests de anonimato

- www.privacy.net Comprueba tu nivel de anonimato y privacidad (bastante fiable)
- www.ip-check.info Comprueba tu nivel de anonimato (bastante fiable)
- www.ip.cc/anonymity-test.php Comprueba tu nivel de anonimato
- www.ip.cc/check-proxy-basic.php El anterior pero en modo texto
- test.anonymity.com Comprueba tu nivel de anonimato

Redes sociales

- www.brizzly.com Maneja varias cuentas de twitter y facebook simultaneamente
- www.twitterfeed.com Difunde automaticamente los contenidos de tu blog a twitter, facebook y más
- www.pixelpipe.com Controla gran cantidad de redes sociales, de blogs, etc... desde una sola página
- www.hootsuite.com Controla varias redes sociales desde una sola página
- www.twitlonger.com Escribe tweets más largos

Texto o código

- www.pastebin.com Comparte texto o código
- www.defuse.ca Igual que el anterior pero encriptado y más herramientas
- www.pastebay.com Más seguro que pastebin, no hace falta loguearse y los posts no son eliminables ni por imperativo legal

Multimedia

- www.aviary.com Completo editor multimedia
- www.masher.com Mezcla videos, música y fotos

Diseño de logos

- www.logomaker.com
- www.onlinelogomaker.com
- www.simwebsol.com/ImageTool

Alojamiento de archivos

- ge.tt
- turbobit.net
- 1fichier.com

Caballeros del lulz: troll /b/astards

Anonymous es la representación del anonimato a través de Internet, donde las personas se muestran completamente libres para actuar y sacan a la luz la verdadera esencia de la Red, abordando ese espacio cibernético con todas las ideas que fluyen en él y por supuesto, pasándolas a través del prisma del humor más irreverente, convirtiendo Internet en un lugar caótico donde todo tiene cabida sin limitaciones de ningún tipo más allá que las de la propia mente humana. Y todo ello surge a partir de un meme creado en el imageboard 4chan, dentro del subforo /b/ frecuentado por los llamados /b/astards, donde se dan cita todo tipo de imágenes aleatorias. Recordad que… "Si algo existe, puede tener una versión pornográfica en 4chan".

Con el paso del tiempo, las ideas de los usuarios de /b/ se centraron en la defensa de la Libertad en la Red dando lugar a una gran conciencia colectiva. Como un panel de abejas, trabajando por un bien común, se formó una masa imparable, ya sea "4 teh lulz" (porque podemos y por diversión) o como método de reivindicación.

El primer paso de Anonymous con una ideología asentada fue en el año 2008 cuando se filtró en YouTube un vídeo de la iglesia de la Cienciología en el que aparecía Tom Cruise. Como respuesta, la iglesia pidió que el vídeo fuera eliminado por violación del copyright y Anonymous entró en acción realizando unos DDOS (ataques de denegación de servicio) contra sus páginas web y convocando protestas a sus puertas por el derecho a la Libertad de Expresión y contra la censura en Internet. Contra todo pronóstico, la Red se hizo manifiesta en las calles marcando un punto de inflexión del que surgiría la Idea de Anonymous tal y como la conocemos hoy.

Lo siguiente es de sobra conocido. La evolución de sus ideas han llegado más allá del ciberespacio y en la actualidad no sólo se defiende la Libertad en Internet: su lucha está enfocada en la consecución de la Libertad en todas sus formas. Lo que distingue a Anonymous de otros movimientos de lucha son las formas, casi todas ellas divertidas. Libres de etiquetas. Libres de límites impuestos por terceras personas. Libres de toda vergüenza. Libres para hacer el ridículo ridiculizando a otros o a un concepto.

Casi nadie nos entiende. Eso nunca nos ha preocupado. Esperamos, querido lector, que éso tampoco te preocupe a tí.

Gracias, terroristas

Sí, ésa es una de lis múltiples etiquetas que nos endosan quiénes no nos comprenden. Es un término tan vago y tan lleno de valores y connotaciones diversas y contradictorias entre sí, que para nosotros nos es indiferente qué significado tenga para determinadas personas.

Para finalizar, sólo nos queda dar las gracias a todos aquellos que han hecho esto posible (¡Gracias, Anonymous!) y a todos los que habéis decidido iniciaros en este camino (¡mucha suerte, Anonymous!).

Aunque en Anonymous adoramos el trolling también trabajamos duro, y muchas veces este trabajo es ilegal. Cuando los de arriba se saltan las normas a nuestra costa resulta estúpido que los de abajo las sigamos cumpliendo. No obstante, la ley persigue a los integrantes de este movimiento y tenéis que ser conscientes de que un canal donde se pretenda reunir a todos los que lo integramos en España como ocurre con los canales de servidores de IRC es la trampa en donde la policía quiere que volvamos a caer. Aprendamos de los errores. Es mucho más seguro que Anonymous trabaje en pequeños grupos de máxima confianza. Recomendamos que estas personas de confianza con ideas claras hagan el esfuerzo de ser autodidactas y mover la información de la forma más sigilosa posible, de manera que las acciones puedan ser mucho más grandes por inesperadas y bien

preparadas. Nadie dijo que el trabajo fuese a ser fácil. Uníos por la vía que deseéis, pero una que sea lo menos pública posible y que, siendo pocos, podáis dedicaros de lleno al trabajo. Demostrado está que los canales públicos de IRC sólo atraen a trolls tanto de la policía como ciudadanos sin vida social, buscad alternativas.
En Anonymous es menester saber desprenderse de las cosas, tanto alias como vías de encuentro, porque esta es la única vía real del anonimato. Un asentamiento es un lugar que puede ser bombardeado; sé un nómada y aprende a moverte por las sombras. Crea confusión y vencerás.
Tener portales como blogs o perfiles de Twitter donde mover la información está muy bien, pero los lugares desde donde se realizan las acciones harán bien manteniéndose en el más puro anonimato.

Es hora de ponerse en serio y entrenarse duro poniendo en práctica el anonimato más feroz.
Trabajad duro en pequeñas células y venceremos. Dispersos pero no divididos, siempre brindándonos apoyo unos a otros. Pues cuanto más dispersos, más confusos los mantendremos. No dejes de leer. No dejes de conocer. No dejes de desconfiar de la autoridad y de los egofags.
Aprende. Crea. Lucha. Ahora y Siempre.

El Conocimiento es Libre
Somos Anonymous
Somos Legión
No olvidamos
No perdonamos
…Y deberíais habernos esperado ;)