

# #OpNewBlood

#anonymous|#CyberHunterOP



#1 Recuerda y guarda esta información

#OpSec:

#2 Nunca filtre datos personales.

#3 Tenga siempre cuidado en línea. Nunca digas cosas que puedan ayudar a otros a encontrarte.

#4 Nunca des información sobre si llueve/hace sol, día/noche en el lugar donde vives. Nunca hables de eventos que estén cerca de donde vives.

Opcional: Si quieres dar información sobre el tiempo, da lo contrario de la verdad. Si está lloviendo, diga que hace sol, etc., o evite responder en absoluto. En algunos casos, dejar pistas falsas puede

Ser una buena opción. Si debes enviar una captura de pantalla de tu Android, evita mostrar la hora/idioma actual visible en la captura de pantalla, ya que alguien podría entender tu hora actual y el idioma que hablas.

#5 EVITE HACER CLIC en ENLACES INNECESARIOS O SOSPECHOSOS, EVITE EJECUTAR ARCHIVOS EN SU SISTEMA SIN ANTES ANALIZARLOS CORRECTAMENTE O HABERLO HECHO EN UN SISTEMA OPERATIVO APARTE (podrían ser secuestradores de IP/phishing, malware). NO ABRA ARCHIVOS SOSPECHOSOS NI INSTALE APLICACIONES SOSPECHOSAS, INÚTILES O INFLUENCIADAS.

Si no está seguro, primero cargue la muestra (video/imagen/documento/software) en

<https://www.virustotal.com/gui/home/upload>, <https://www.bybrid-analysis.com/>, <https://www.joesandbox.com/#windaves> y muchos otros. Aún así, es posible que no se detecten algunas aplicaciones maliciosas. NOTA: en caso de que su dispositivo presente síntomas anómalos, como lentitud constante, o si sus redes sociales notifican alertas, se publica sin permiso o han perdido el acceso, haga una revisión INMEDIATA de su pc o celular, y acostúmbrese a hacerlo todos los días. Se le recomienda utilizar: para po

<https://es.malwarebytes.com/premium/> para celular

<https://es.malwarebytes.com/android/>

#6 Si es posible, utilice un número de grabadora para iniciar sesión en aplicaciones de redes sociales o cualquier otra cosa, como Telegram o Signal.

Asegúrese siempre de utilizar contraseñas seguras (al menos 16 caracteres. Letras mayúsculas, letras no mayúsculas, caracteres especiales y números), y sería bueno configurar 2FA siempre que sea posible.

Cuando NO NECESITE el número de quemador o el teléfono de quemador, apáguelo. Saca la batería y la SIM | Si es posible, colócalo dentro de una jaula de Faraday o simplemente apágalo y déjalo en un lugar seguro.

La próxima vez que lo necesites, enciéndelo nuevamente y sácalo de la caja.

Opcional pero seguramente podría ayudar: cubrir las cámaras con cinta adhesiva.

Los teléfonos desechables y los números desechables también se pueden utilizar para realizar OSINT y registrar cuentas en línea. Asegúrate de crear perfiles falsos muy atractivos (LinkedIn, Facebook, Instagram, Twitter, Reddit o cualquier sitio en el que quieras registrarte).

Utilice This PersonDoesNotExist u otros sitios web y genere algunos nombres e identidades falsos.

Evita que tus contactos reales que conoces en la vida real aparezcan en perfiles tan falsos. Evite sincronizar sus contactos en sus perfiles sociales falsos.

Desde un teléfono desechable o un número desechable, evite realizar llamadas a contactos que conoce en la vida real. Nunca almacene información personal/contactos/detalles de la vida

En teléfonos desechables.

#7

Computadora portátil/PC:

Evite el uso de sistemas operativos de código cerrado (MAC/Windows)

Cubra cámaras y micrófonos si los hay, en caso de que no los estés

Usando.

Cifre el disco duro y los dispositivos de almacenamiento utilizando LUKS o algo más confiable.

Utilice contraseñas seguras para el cifrado de dispositivos de

Almacenamiento y para las cuentas de usuario. ¡EVITE UTILIZAR LA MISMA CONTRASEÑA UNA Y OTRA VEZ! Utilice Linux como sistema operativo en caso de abrir archivos, entrar en reuniones, o demás situaciones que puedan revelar su identidad o infectar su ordenados.

Si desea utilizar Windows, úselo en una máquina virtual y limpie/restaure la máquina virtual cada cantidad de días/semanas. No utilice una licencia y evite instalar software sospechoso en ella. Recuerda que puedes usar BleachBit para triturar archivos que quieras eliminar por completo, ¡lo que dificulta su recuperación! (Pero no imposible. Lea sobre ciencia forense digital y temas relacionados para comprender más al respecto). Lo mismo ocurre con Linux. Utilice BleachBit o triture. Recuerde que si utiliza SSD o hardware nuevo, puede resultar más difícil borrar archivos de forma segura.

Recuerde utilizar exifcleaner para eliminar metadatos exif de fotos, vídeos y archivos similares.

Si debe borrar por completo el dispositivo o un disco duro, etc., destrúyalo y asegúrese de que sea difícil recuperar cosas de ellos. Normalmente un taladro hace el trabajo.

#8

Android

Evite el uso de iPhones (si es posible). Opcional: asegúrese de cubrir cámaras y micrófonos, en el caso de no hacer uso de ellos, por decirlo de un mejor manera, NO DEJE PUERTAS ABIERTAS.

Utilice Android (Graphene OS si es posible). Desgooglee su teléfono si no puede usar el sistema operativo Graphene y desbloquéelo (elimine las aplicaciones incluidas y los servicios de Google de su teléfono).

Recuerde que los teléfonos se utilizan para hacer llamadas y cosas así. Nunca los uses para hacer nada ilegal.

Nunca te tomes fotografías. Si toma una fotografía de un lugar, asegúrese de que no sea fácil entender dónde está ese lugar en el mundo (bastante difícil) y borre los metadatos exif de la foto. Asegúrese de nunca publicar este tipo de fotos en línea. Y hagale un favor a la humanidad, NO PUBLIQUE FOTOS DE SUS HIJOS Y NIÑOS EN GENERAL, LOS PEDERASTAS TAMBIEN SABEN RASTREAR!

Si debes borrar completamente Android, puedes optar por destruirlo (Drill). Quitando la batería primero, podrías evitar hacerte daño.

#9

## Mensajería Instantánea

Sesión: No requiere una dirección de correo electrónico ni un número de teléfono.

Señal: Requiere un número de teléfono. Vea si puede utilizar servidores proxy o enrutar su tráfico a través de nodos TOR. Utilice un número que no esté asignado a usted

Telegram: utiliza chats secretos. Evite enviar imágenes/realizar llamadas. Vea si puede utilizar servidores proxy para enrutar su tráfico (nodos TOR).

#10 Servicios de correo electrónico: ProtonMail: utilice correos electrónicos falsos y contraseñas seguras. Se sugiere crear una cuenta e iniciar sesión sólo desde

TOR, una VPN o un proxy. Tutanota: Lo mismo que se dijo anteriormente para ProtonMail debe tenerse en cuenta aquí para Tutanota

#11

Monero y otros:

Utilice Monero para pagar Mullvad VPN y otros servicios en línea. Si tienes que comprar algo en la vida real, usa sólo efectivo. Evite las tarjetas de crédito o compre tarjetas prepagas en efectivo.

#12

Navegadores:

Librewolf (Utilice complementos como UBlock Origin, Clear Cookies, User-Agent Switcher y similares). Librewolf podría dar algunos

Problemas al mostrar algunos contenidos en algunos sitios web. Si esto sucede, puedes considerar cambiar a Firefox.

Firefox (Utilice los mismos complementos mencionados anteriormente). Brave (Menos centrado en la privacidad que los navegadores

Anteriores. Está basado en Chromium. En el pasado se detectó utilizando enlaces de afiliados).

TOR (Lento pero seguro).

Navegador Mullvad (Menos seguro que TOR).

#13

VPN:

Mullvad (Pagar con Monero)

ProtonVPN (Menos seguro que Mullvad. Evite usarlo si puede). Si realmente quieres estar lo más seguro posible, utiliza Mullvad VPN. No uses VPN crackeadas, VPN gratuitas ni cosas así

#34

Proxies (Utilice proxies anónimos o proxies privados): Utilice cadenas de proxy (TOR y proxies). Hay muchos sitios que comparten servidores proxy gratuitos, pero tenga en cuenta que pueden registrar su tráfico y lo que hace.

TOR Utilice una configuración segura y mejore la configuración. Si desea estar más seguro, use Qubes OS/Tails/Whonix en una VM o use un USB para usar TOR

#15

Ya sea que esté utilizando Tails, VPN, TOR o proxies, asegúrese de no filtrar DNS ni nada más! Si es así, primero debe corregir estas filtraciones para poder navegar

De forma privada. (No dudes en probar Qubes OS, Tails y Whonix para descubrir cuál funciona mejor para ti. Recuerda que puedes colocarlos en un USB de arranque para usarlos en cualquier computadora portátil/PC).

Incluso puedes configurar tu propia VPN tú mismo. Evite cualquier VPN patrocinada por personas, como si fueran las mejores cosas jamás creadas. No lo son y dan datos a los gobiernos.

Antes de confiarle a alguien o algo su tráfico e información, investigue mucho sobre ellos (la empresa). Mire a su alrededor para ver si alguna vez entregaron registros a

agencias, auditorías, si alguna vez fueron violados y si el director ejecutivo y otras personas importantes de la empresa tienen dudas.

#16

TOR

Recuerde que los gobiernos también tienen nodos TOR. Puede decidir cambiar su IP actual cada pocos minutos. Nunca inicie sesión en sus cuentas reales y correos electrónicos desde una cuenta creada en TOR o en un teléfono desechable. Esto comprometerá su verdadera identidad.

#17

Administradores de contraseñas:

KeePass Encuentre administradores de contraseñas de código abierto, que hayan tenido auditorías y que sean confiables.

Evite escribir todas sus contraseñas dentro de un archivo de texto y guardarlo en el escritorio (Obviamente). Puede considerar almacenar todos sus correos electrónicos y contraseñas en un USB cifrado o en una hoja de papel bien oculta (si es adecuado), pero esa podría no ser la mejor solución y podría crear nuevas amenazas a su privacidad, y seguridad. Por lo general, depende de cuál sea su módulo de amenaza.

#18

10:

Cifrado:

VeraCrypt

Cripta verdadera

Mejor Cripta

7Zip

#19

Redes sociales y cuentas:

Evite utilizar 1 correo electrónico para todo. Crea 2/3 (o incluso más) y usa cada uno de ellos para diferentes propósitos, según lo que quieras hacer con ellos.

Si es posible, evite iniciar sesión en todos sus correos electrónicos desde el mismo dispositivo, ya que esto podría usarse para demostrar que usted es el propietario de dichas direcciones de correo electrónico. Probablemente se registrará la IP que utilizó para crear e iniciar sesión en sus cuentas, lo que dará prueba de que usted es efectivamente el propietario de dichas cuentas.

Evite verificar cualquiera de sus cuentas con su número de teléfono real. Utilice otro número.

- Evite usar el mismo apodo/identificador/imagen de perfil en todas partes. Con una única búsqueda en Google, cualquiera puede encontrar todos sus perfiles y cuentas en línea.

Made by: @CyberHunterCO