SEGURIDAD DIGITAL EN TIEMPOS DE VIGILANCIA

Te presentamos la guía básica para conexión en Internet de forma segura en tiempos de vigilancia y censura. Aprende a buscar, recibir y difundir información reduciendo las posibilidades de ser identificadx, además de evadir bloqueos de páginas web y proteger la información que llevas contigo en los dispositivos móviles.

Contenido:

PRIMEROS PASOS

Antes de darte tips puntuales es necesario que tengas en cuenta recomendaciones básicas que van a aumentar tu seguridad digital en el día a día, no deben faltar en tu protocolo de seguridad digital, son fáciles de poner en práctica y gratuitas.

- En todas tus cuentas y dispositivos: utilizar **contraseñas seguras**, con más de 25 caracteres alfanuméricos y especiales, que incluyan mayúsculas y minúsculas. Una manera de crearlas (y recordarlas) es utilizar una frase y sustituir letras por números o caracteres especiales; por ejemplo, de "pabelloncriollo" a "Pab3l#onCr1o#o"
- En tus correos: **verificación de doble paso.** Permite tener una capa más que tu contraseña para ingresar a tu correo, a través de un código que recibes en tu teléfono celular o en el de una persona de confianza. Puedes configurar teléfonos de emergencia y descargar una lista de códigos de uso único por si no puedes acceder a través de tu dispositivo móvil. También puedes activar este mecanismo de seguridad en tu cuenta de Twitter y Facebook.
- **Manejador de contraseñas**: Funciona como una caja fuerte en la red, encriptada y organizada por carpetas. Recomendamos LastPass, ya que es multiplataforma y fácil de utilizar. La herramienta también permite compartir claves de manera segura con contactos de confianza, tiene un generador de claves seguras, y autocompleta los formularios con tus claves, lo que permite evadir malwares que roban tu identidad leyendo lo que tipeas desde tu teclado.
- **Antivirus actualizado**: para evitar la instalación de software maligno en tus dispositivos. Puedes instalar Avast en tu computadora y AGV como aplicación para dispositivos móviles.

EN EL DÍA A DÍA

1 No compartas tus contraseñas: no sabes en qué momento pueden dejar tu cuenta abierta en su computadora o en un equipo de uso público, cómo guardan y protegen esa clave, o si la facilitan a otra persona.

2 No publiques en tus redes sociales información que pueda ser utilizada para responder a tus preguntas de seguridad: nombres de familiares, mascotas, colegio...

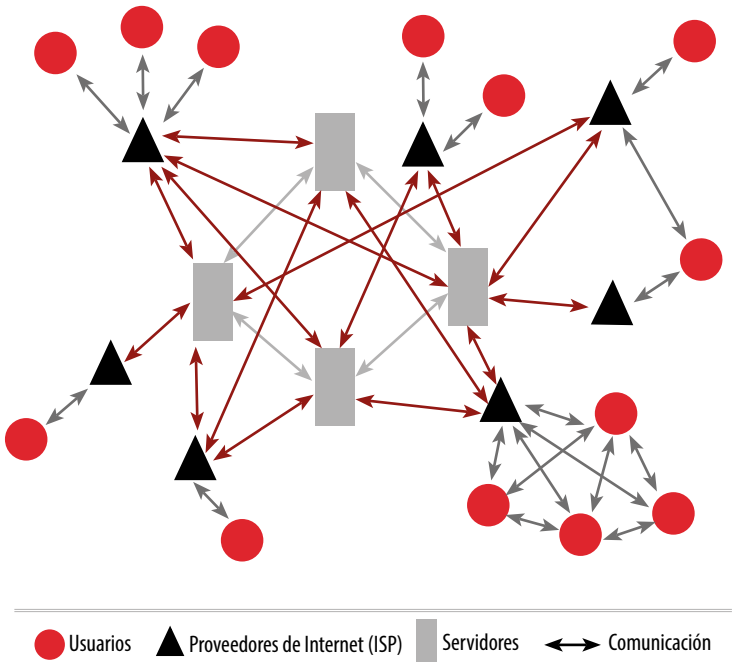
3 Siempre que te conectes desde un cyber o desde una computadora prestada, navega en modo incógnito

4 Mantén apagado el Bluetooth, Wi-fi y GPS de tu teléfono celular mientras no los necesites

5 Acostúmbrate a cerrar sesión de tu correo y redes sociales antes de apagar el equipo, esto puede evitar que intervengan tus cuentas si roban tu computadora

espacio público

www.espaciopublico.ong
Twitter: @EspacioPublico
Instagram: @ONGEspacioPublico
Facebook: EspacioPublico



¿Cómo funciona Internet?

Esta herramienta trabaja como una red internacional que tiene millones de usuarios, proveedores de servicio, y servidores que almacenan la información. Cada usuario y sitio web tienen una identidad única: la IP. A través de este número se identifica cada parte de esta red y se transmite y recibe información.

Usuarios y sitios web están conectados entre sí, pero para poder comunicarse requieren un proveedor de servicios de Internet (ISP por sus siglas en inglés): quien envía los datos de un punto a otro. Además, puede haber redes internas en las que varios usuarios están conectados entre sí, como las utilizadas en oficinas u hogares.

En este proceso el proveedor de Internet conoce quién solicita la información, a quién, y cuál información, simplemente a través de las IP y la solicitud del paquete de datos.

Adicionalmente, la información entre el usuario y el ISP, dependiendo de la página que se visite está o no cifrada, por lo que cualquier persona puede interceptar esa comunicación y acceder al paquete de datos que se reciben o envían.

ANONIMATO: TOR

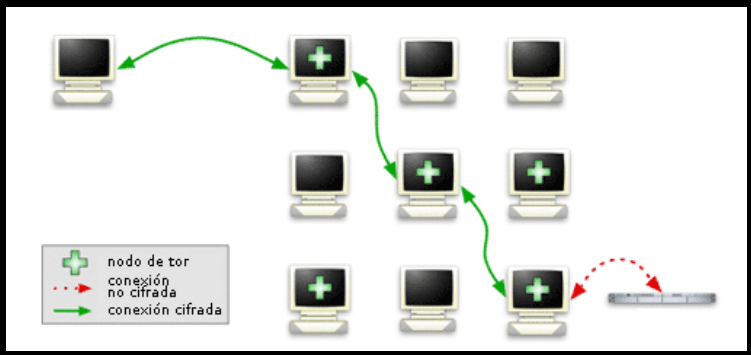
A través de la dirección IP es posible identificar quién o desde dónde se publicó una información; por lo tanto, es necesario que al colgar información en nuestra página web, lo hagamos de forma segura, escondiendo nuestra identidad.

Para esto, la mejor herramienta gratuita y fácil de usar es TOR, un explorador de internet con tres nodos de IP antes de hacer la solicitud a tu ISP. Se puede descargar en https://www.torproject.org/ y utilizarlo como Chrome o Firefox, pero resguardando nuestra identidad. Además, Tor permite evadir los bloqueos de páginas web que son exclusivos a usuarios venezolanos, aplicados por ABA y por otros proveedores de Internet.

La red de Tor funciona con personas que hacen de sus computadoras servidores que permiten hacer una conexión indirecta con tu ISP y evita que se conozca que eres tú quien ingresa a una página web. A través de una comunicación codificada entre cada nodo, puedes ver la página que deseas mientras evitas que se sepa cuál información solicitaste.

Sólo el último punto de la conexión al servidor que contiene la información que estás solicitando es el que conoce qué paquete de datos se requieren (por ejemplo, Gmail o redes sociales), sin identificar que eres tú quien necesita acceder. Al obtener la información, es enviada de regreso al usuario de Tor a través de tres nodos diferentes a los iniciales, en una comunicación encriptada hasta el último punto antes de la entrega a tu IP.

Sigue los enlaces para más infromación para Windows o Linux



PRIVACIDAD: VPN

El VPN (Virtual Private Network) es una red privada virtual que oculta cuáles son los datos que se transmiten: identifica las IPs pero resguarda la información que se recibe, y la envía creando un túnel privado en Internet, entre tu dispositivo y el servidor VPN, por lo que no es posible ver los datos encriptados que se transmiten.

Por ejemplo: entre dos islas (dispositivos personales y servidores), hay mar (Internet), a través del cual deben pasar las personas (datos), para ir de un sitio a otro. La vía tradicional para viajar de un punto a otro son barcos, y los funcionarios de cada isla saben quién se sube y se baja de los barcos. El VPN sería como crear un túnel bajo el agua, de cristales ahumados, a través del cual pueden moverse las personas (datos) sin pasar por migración, y sin que nadie las vea.

Recomendamos el uso de Hola! Una extensión para Google Chrome que puedes descargar e instalar desde este enlace. Para dispositivos móviles, Firefox, Apple u otros sistemas operativos puedes descargar la aplicación gratuita que corresponda en http://hola.org/

Para ver, descargar y utilizar otros VPN, puedes revisar este enlace.

Privacidad + anonimato

Para conseguir ambos beneficios, conéctate primero a través de un VPN y luego navega con el buscador TOR

ELIMINAR INFORMACIÓN DE FORMA SEGURA

En caso de almacenar datos delicados en nuestros dispositivos, es necesario saber que cualquier persona con conocimientos informáticos puede acceder a esos archivos, por lo que debemos ser muy cuidadosos con la información sensible que almacenamos; por ejemplo, fotos personales, archivos, listas de contacto y ubicación de familiares, amigxs o víctimas, nómina de personal, rendición de proyectos, entre otros.

¿Qué pasaría si esa información cae en manos no deseadas? ¿Si es publicada en Internet? Exponer a víctimas en riesgo o a contactos importantes no es una decisión deliberada; sin embargo, **al borrar archivos de nuestros dispositivos siempre queda rastro** de las versiones anteriores y sigue disponible el original, sólo que su nombre es "borrado" del archivo de la computadora o celular, pero los documentos siguen en el disco duro.

Para borrar definitivamente los documentos, es necesario utilizar herramientas especiales que garantizan la eliminación de copias y versiones anteriores. CCleaner y Bleach.bit son dos opciones confiables.

Antes de empezar....

Las configuraciones predeterminadas de tu sistema operativo o un navegador web crean una recopilación de datos que puede ser interceptada por expertos malintencionados. Cada vez que utilizas un navegador web o un procesador de texto, vas generando y almacenando archivos temporales. También puede incluso generar listas de documentos o páginas web recientes. Por ejemplo, cuando empiezas a teclear un sitio web en tu navegador, probablemente verás aparecer una lista de aquellos sitios web visitados recientemente que empiezan con las mismas letras.

Después de utilizar CCleaner, perderás el historial de navegación, el historial de documentos recientes e incluso tus contraseñas guardadas. Sin embargo, este es precisamente el objetivo de esta herramienta, minimizar las posibilidades de infectar o monitorear tu computadora.

Instalación:

- Entra en http://www.piriform.com/ccleaner/builds Haz clic en el ícono de CCleaner para abrir la página de descarga
- En la sección 'CCleaner - Slim', haz clic en el botón 'Download' (Descargar)
- Lee las 'Instrucciones de instalación' antes de continuar
- Guarda el archivo 'ccsetup_slim.exe' en tu computadora, luego búscalo y ábrelo
- Después de instalar correctamente CCleaner, elimina el archivo de instalación de tu computadora
- Configúralo como recomiendan en este enlace.

DISPOSITIVOS MÓVILES

Los teléfonos móviles se han convertido en una herramienta de comunicación omnipresente y básica — hoy son usados no solamente para hacer llamadas, sino también para acceder a la Internet y enviar mensajes de textos y documentos al mundo.

Desafortunadamente, los teléfonos móviles no fueron diseñados para la privacidad y seguridad. No solamente hacen un pobre trabajo para proteger tus comunicaciones, ellos también te exponen a un nuevo tipo de riesgo en la vigilancia, especialmente en el rastreo de localización. Las recomendaciones presentadas en cada caso también funcionan en dispositivos que tengan Wi-Fi y/o Bluetooth.

Confiscación o robo

Es fundamental tomar previsiones en caso de exponerse a una situación donde tu teléfono o equipo móvil puede ser confiscado por las autoridades locales. Usualmente un análisis forense puede sobrepasar cualquier forma simple de bloqueo de pantalla, o que permitiría acceder a la información almacenada en tu teléfono (contactos, imágenes, audio, textos); incluso recuperar archivos que han sido borrados previamente. De estar disponible, activa el cifrado de tu teléfono en la configuración de seguridad del dispositivo; esto dificultará el acceso a la información a especialistas.

Recomendaciones

- Instala en tu teléfono una aplicación que permita borrar archivos de forma remota.
- Mantén respaldos automáticos en la nube, evitar perder imágenes o videos hechos realizados en cobertura periodística o trabajos de campo.
- Vacía los chats de mensajería instantánea que utilices, eliminando mensajes y archivos almacenados en tu teléfono.
- Realiza un borrado seguro frecuentemente.
- Mantén actualizado el antivirus

Rastreo de ubicación

La mayor amenaza es cómo los teléfonos anuncian tu ubicación todo el día (y toda la noche) a través de las señales que envían. Hay por lo menos cuatro maneras en que un teléfono celular puede ser rastreado por otros:

1 Por triangulación de la operadora de servicios, siempre que el teléfono esté encendido y conectado al proveedor de telefonía. Puede llegar a tener un margen de error de seis metros. El Estado puede acceder a esa data forzando al operador a facilitarla.

2 IMSI Catcher: (International Mobile Subscriber Identity), a través de un dispositivo trasladado a la zona, una persona puede conocer el identificador único de la tarjeta del teléfono fingiendo ser una torre de telefonía móvil.

3 Wi-Fi y Bluetooth: siempre que estén encendidos, emitirán señales periódicamente, éstas son identificadas por un serial único llamado MAC y así se puede conocer si el dispositivo (o su dueño) estuvo en un lugar específico. Los operadores de una red Wi-Fi también pueden ver la dirección MAC de cada dispositivo que se una a su red, lo que implica que pueden reconocer un dispositivo en particular en un tiempo dado y deducir si eres la misma persona que se unió a su red anteriormente.

4 Aplicaciones y navegadores web: Hay apps que solicitan acceder a tu ubicación para proveer correctamente el servicio que ofrecen (como mapas, tráfico); además pueden transmitir tu localización a través de la red del proveedor de servicios, el cual a su vez, la entrega a otras personas que te siguen a tí. Por ejemplo, el rastreo de localidad puede ser usado para saber si una persona atiende a una

reunión en particular, una protesta, o tratar de identificar cuál era la fuente de información confidencial de un periodista.

¿Cómo cuidarnos?

En caso de que sepas que tus movimientos estén siendo vigilados puedes tomar varias precauciones:

- Revisar qué aplicaciones tienen acceso a tu ubicación, desactiva las que no te den confianza
- Mantener apagado el Wi-Fi y el Bluetooth
- No llevar ningún dispositivo móvil a reuniones o lugares donde vas a intercambiar información sensible
- Apagar el celular y retirar la pila mientras te estés trasladando al sitio o cuando vayas a tener una conversación confidencial. Se han detectado malwares que simulan un falso apagado y pueden seguir utilizando la cámara y voz del teléfono siempre que la batería esté colocada.
- Utilizar varios teléfonos prepagados cuyo SIM card no esté relacionad contigo. Cambiar frecuentemente el SIM y el equipo, ya que ambos están asociados y puede registrarse también el IMEI o identidad única de un teléfono al utilizar un SIM. Evita llamar desde esos números a contactos frecuentes, ya que podrías ser identificadx.

Espionaje durante llamadas y SMS

Cualquiera con un sistema de radio correcto podría escuchar las llamadas e interceptar mensajes de texto. Igualmente, los operadores de móviles tienen la habilidad de conocer y grabar toda la información sobre quien llamó o quien envió texto a quién, cuándo, y qué se dijo.

¿Cómo cuidarnos?

La práctica más segura es asumir que las llamadas tradicionales y los mensajes de textos SMS no han sido aseguradas contra la escucha o las grabaciones. Para comunicaciones sensibles, procura llamar a través de aplicaciones que contemplan el cifrado, como Signal, Telegram, Whatsapp, Wickr Me, Facebook Messenger y Viver (activando las opciones de cifrado). Puedes ver más opciones en este enlace.

espacio público
www.espaciopublico.ong
Twitter: @EspacioPublico
Instagram: @ONGEspacioPublico
Facebook: EspacioPublico