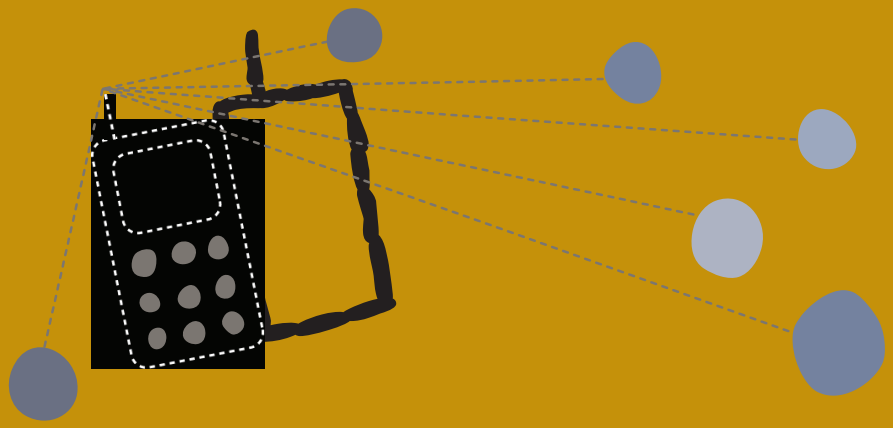
Seguridad y privacidad móvil y en línea



LAS NUEVAS TECNOLOGÍAS, TALES COMO LOS TELÉFONOS MÓVILES E INTERNET, SON PODEROSAS HERRAMIENTAS PARA LAS ACTIVIDADES DE DEFENSA DE LOS DERECHOS HUMANOS, PERO SU USO PARA COMUNICAR INFORMACIÓN SENSIBLE PUEDE GENERAR RIESGOS PARA USTED, SUS CONTACTOS, AMIGOS, AMIGAS Y COLEGAS. ESTA TARJETA LE AYUDARÁ A ACCEDER A INFORMACIÓN DE FORMA SEGURA Y PROTEGER SUS DATOS CUANDO UTILICE TELÉFONOS MÓVILES E INTERNET.

¿QUÉ ES LA SEGURIDAD Y LA PRIVACIDAD DIGITAL?

Entre los indicios que señalan que se ha comprometido el derecho a la información y la seguridad digital, se podrían incluir los siguientes:

- Contraseñas que cambian de forma misteriosa
- Mensajes privados que pareciera que alguien que no es el destinatario o la destinataria los ha leído
- Páginas de Internet de ciertos países que ya no son accesibles
- Funcionarios o funcionarias que revelan su conocimiento sobre correspondencia privada, lo que incluye fechas, nombres o asuntos y temas discutidos
- Conversaciones por teléfono celular que algunas personas creen que se han monitoreado

¿ME DEBE PREOCUPAR ESTO?

Si estas situaciones comprometen sus proyectos o exponen a sus contactos al peligro de la persecución, entonces sí deben preocuparle. Con frecuencia, el conocimiento y los programas de cómputo necesarios para llevar a cabo tales ataques a su privacidad digital están disponibles en Internet. Si el o la atacante tiene acceso suficiente a la infraestructura de los teléfonos móviles o de Internet de su país, la tecnología necesaria es bastante sencilla. Las agencias gubernamentales, los Proveedores de Servicios de Internet y las empresas

de telefonía móvil tienen acceso privilegiado a esta infraestructura, pero los compañeros/compañeras de trabajo, los vecinos/vecinas y los encargados/encargadas de los cafés Internet también podrían tener cierto acceso a la información.

¿QUÉ ASUNTOS DE SEGURIDAD ABARCA ESTA TARJETA?

Esta tarjeta hace énfasis en las herramientas basadas en Internet y en los teléfonos móviles. Sin embargo, hay muchas otras tecnologías que también pueden permitir que usted sea vulnerable a la censura, la vigilancia y la persecución. Si bien éstas no se exponen en esta tarjeta, la actualización regular del sistema operativo de su computadora, un programa de cómputo confiable contra los virus informáticos o software malicioso (malware) y procedimientos consistentes de respaldo son algunas de las medidas más importantes de precaución. Si usted tiene alguna razón para creer que su computadora o sus dispositivos para el almacenamiento de información, lo que incluye sus archivos de respaldo, corren el riesgo de que se pierdan, los roben o los confisquen, o que su organización podría estar sujeta a algún tipo de vigilancia en Internet (o si esto es algo común en la región donde trabaja), deberá referirse al conjunto de herramientas denominado "Security-in-a-box" que ha desarrollado Tactical Tech.

Herramientas de Internet para la defensa de derechos

Cuando utilice herramientas en Internet, tales como Blogger, Facebook y Twitter, para propósitos de movilización o de coordinación, recuerde que la información que se almacena en este tipo de plataforma pasa a ser, hasta cierto punto, propiedad de los encargados o encargadas de estas páginas y que muchas de estas herramientas dejan al descubierto más información de la que usted podría pensar. Cuando usted confíe un proyecto de índole sensible a los operadores o las operadoras de cualquier herramienta en línea, lea sus políticas de privacidad o los acuerdos de usuario. Recuerde que hasta la política más progresista deja la información que usted publique bajo el control directo de los administradores o administradoras de la plataforma, los y las cuales pueden divulgar, vender o extraviar esa información sin su permiso o conocimiento. Aun si usted cancela su cuenta, muchas de estas páginas no borran el contenido que usted ha publicado o la información personal que ha suministrado. Finalmente, a menos que sea importante que usted utilice un servicio comercial en particular, ya sea debido a su accesibilidad o porque al hacerlo puede integrarse a los usuarios y las usuarias con menor notoriedad, tome en consideración algunas de las alternativas progresistas en cuanto a los derechos, tales como Blip.tv en vez de YouTube o Riseup.net en vez de Gmail. Si cuenta con recursos técnicos, usted puede administrar sus propios servicios basados en Internet.

Si utiliza plataformas comerciales, tome precauciones para protegerse de personas maliciosas que saben cómo descubrir información privada en estos servicios. Esto es particularmente común en plataformas de redes sociales tales como Facebook y MySpace. Familiarícese ampliamente con las funciones de privacidad que incluyen estas plataformas y piense en el tipo de información que usted podría revelar involuntariamente sobre usted o su organización; por ejemplo, su nombre verdadero, dónde vive, los lugares a los que viaja y detalles sobre sus próximas actividades o reuniones. Si se sigue de cerca durante mucho tiempo, esta información también puede ofrecer una idea de los hábitos y las prácticas de trabajo que usted aplica.

Una técnica útil es crear varias cuentas en cualquier servicio por Internet, lo que le permite utilizar diferentes perfiles o cuentas para distintos proyectos y mantener cuentas de prueba que usted puede usar para 'espiarse' a sí mismo(a). Su privacidad está mejor protegida si usted puede verificar, de diferentes formas, lo que se revela sobre su cuenta; por ejemplo, a través de búsquedas en Internet o personas que tienen privilegios especiales de acceso.

CONTRASEÑAS

La mayoría de los recursos en Internet dependen de una sola contraseña para proteger su cuenta. Si una persona u organización malintencionada

descubre esta contraseña -sin importar si confía en los administradores o las administradoras de la página de Internet o con qué cuidado ha verificado su privacidad -usted perderá inmediatamente su confidencialidad y anonimato.

Hay otras formas menos conocidas para descodificar una contraseña: alguien podría instalar algún software malicioso en una computadora que usted usa para ingresar a una página segura de Internet.

Para protegerse contra este primer tipo de ataque, utilice su propia computadora o una cuyo mantenimiento esté a cargo de alguien en quien usted confía y cerciórese que tanto el sistema operativo como el software contra este software malicioso están actualizados. Para protegerse contra el segundo tipo de ataque, las plataformas más populares de correos electrónicos, redes sociales, blogs, mapeo y videos en Internet ofrecen conexiones seguras denominadas HTTPS. Usted puede verificar si tiene una conexión segura con una página de Internet al buscar 'https://' (en vez de sólo 'http://') al principio de la barra de direcciones de su explorador. Sin embargo, muchas de las herramientas en Internet no utilizan HTTPS para proteger cualquier tipo de información que usted incluya o acceda desde esas páginas, a excepción de su contraseña. En consecuencia, si alguien monitorea su conexión durante suficiente tiempo, podrá descubrir lo que usted ha almacenado en esa página de Internet. Su mejor defensa en contra de esto es buscar herramientas en Internet que utilicen HTTPS en todas las páginas.

PARA ELUDIR LA CENSURA

Usted puede utilizar programas seguros que permiten que varias computadoras ingresen a Internet a través de una sola conexión física (denominados "proxies"), al igual que herramientas para eludir la censura y programas de cómputo para mantener su anonimato, tal como el programa Tor, a fin de ocultar su identidad en las páginas de Internet que visita o de eludir los filtros de Internet. Estas herramientas son útiles para acceder a páginas de Internet que están bloqueadas, por ejemplo, para propósitos de investigación, o para incluir actualizaciones en plataformas de Internet, como Facebook.

PARA MANTENER SU ANONIMATO EN LÍNEA

Los programas de cómputo (software) como Tor son útiles cuando usted no desea revelar cuáles son las páginas de Internet que ha visitado. Tor "rebota" su conexión entre diferentes computadoras que se prestan voluntariamente para evitar que hasta su proveedor de servicios de Internet, observadores u observadoras gubernamentales sepan qué ha estado haciendo en Internet. Sin embargo, no utilice Tor cuando envíe o reciba información sensible hacia o desde páginas de Internet que sean inseguras. A menos que esté conectado o conectada a una página de Internet que utiliza HTTPS, es posible que una de las computadoras "voluntarias" monitoree el contenido a medida que se van cargando los archivos. Aunque Tor es bastante seguro, uno de los aspectos negativos, por el momento, es que reduce la velocidad de su conexión de Internet.

Teléfonos móviles

Los defensores y las defensoras de distintas causas en todo el mundo utilizan teléfonos móviles y por lo general almacenan una gran cantidad de información que debe mantenerse en privado. Además de las listas de contactos, un teléfono móvil puede contener información sobre las llamadas, calendarios, mensajes de texto y correos electrónicos. Piense en la información almacenada en su teléfono, especialmente porque estos se confiscan con facilidad. Por ejemplo, probablemente usted no necesita incluir a todos sus contactos en su teléfono móvil si está llevando a cabo labores delicadas de defensa de derechos y, siempre que pueda, deberá borrar información de su teléfono y de su tarjeta de módulo de identificación del suscriptor (tarjeta SIM, por sus siglas en inglés). Cuando esté organizando actividades o movilizando sus redes, es mejor que utilice tarjetas SIM anónimas y prepagadas y que cambie de teléfono de vez en cuando. Debido a que los servicios de mensajes de texto (SMS, por sus siglas en inglés) pueden localizarse y filtrarse fácilmente, evite el uso de palabras

clave de índole sensible cuando envíe mensajes de texto. En tanto estén encendidos, los teléfonos celulares pueden utilizarse para rastrear su ubicación física. Las personas que asistan a reuniones de naturaleza sensible deben apagar sus celulares y quitarles las baterías antes de dirigirse al punto de reunión y esperar hasta haberse ido para colocar nuevamente las baterías y encender los teléfonos. Los proveedores de telefonía móvil tienen acceso a ciertos detalles sobre las llamadas: a quién, cuándo y dónde se hicieron. Estas empresas también podrían tener la obligación jurídica de registrar o de revelar estos detalles si las autoridades así lo solicitan y pueden mantener estos archivos durante varios años.

ACTIVIDAD: IDENTIFICANDO SUS RIESGOS DE SEGURIDAD

Utilice las siguientes afirmaciones para evaluar los riesgos a su seguridad y para ayudarle a decidir qué herramientas puede utilizar para mitigar estos riesgos.

1. Está trabajando con información sensible. Es importante saber si usted está manejando información sensible que podría despertar el deseo de otros y otras de vigilar lo que está haciendo. ¿Está participando en actividades que el gobierno, la policía o una empresa privada podrían considerar como sensibles o perturbadoras? De ser así, usted podría estar poniéndose a sí mismo y a otros y otras en riesgo, a menos que aplique ciertas medidas de seguridad.
2. Trabaja con personas cuyas identidades y datos personales deben mantenerse en privado. Quizás usted esté recopilando información privada de las personas a quienes apoya, como información sobre violencia doméstica, trabajo forzoso o alguna violación. Si las personas le ofrecen información que las podría poner en riesgo, usted debe tomar las medidas necesarias para velar por que estos datos se mantengan en privado.
3. Algunas veces se comunica en línea con personas que manejan información sensible. Si aún cree que no corre riesgos de seguridad y se comunica con personas que sí enfrentan estos riesgos, usted también puede convertirse en el blanco de aquellas personas que se oponen a lo que están haciendo. Ello obedece a que la gente puede utilizarlo o utilizarla para acceder a la información privada de otros u otras.
4. Ve o publica contenido en páginas de Internet que podría considerarse como sensible. Quizás usted contribuye con información a las páginas de Internet de derechos humanos o publica artículos en los que se opone a grupos que usted cree que no están respetando los derechos humanos. El simple hecho de visitar páginas sensibles en Internet pueden convertirlo o convertirla en un blanco.

Recursos relativos a la seguridad y la privacidad en Internet

Para aprender más y descargar herramientas de seguridad:

1. **Security in-a-box** fue creado por Tactical Tech y Front Line para satisfacer las necesidades de privacidad y seguridad digital de los y las activistas y los defensores/defensoras de derechos humanos. http://security.ngoinabox.org
2. **Seguridad y privacidad digital para los defensores y las defensoras de derechos humanos**, creado por Front Line, ofrece información sobre la forma de evaluar y abordar diversas amenazas digitales. http://bit.ly/1aCkSs (www.frontlinedefenders.org)
3. **Mobiles in-a-box** fue creado también por Tactical Tech e incluye toda una sección sobre la privacidad y la seguridad de los teléfonos celulares. http://mobiles.tacticaltech.org/security
4. **Publicación de blogs con los programas Wordpress y Tor**. Global Voices creó esta guía para apoyar a los defensores y las defensoras de derechos que deseen revelar la verdad y expresarse en línea pero que podrían correr riesgos al hacerlo. http://advocacy.globalvoicesonline.org/projects/guide
5. **Mantenimiento del anonimato en línea y formas de eludir la censura**. El programa Tor está diseñado para aumentar el grado de anonimato de sus actividades en Internet y también puede utilizarse para eludir los filtros de Internet. Usted puede descargar el archivo en su computadora o hacerlo funcionar mediante un dispositivo de memoria USB. http://www.torproject.

versión en español
adaptada por: REDES
TACTICAL TECHNOLOGY COLLECTIVE