espacio público

Guía de seguridad digital para activistas y defensores de derechos humanos

Internet es una herramienta potencial para la defensa y promoción de los derechos humanos, su uso ha permitido a los activistas y defensores ampliar sus redes de divulgación, su interacción con las personas y establecer contactos con aliados, todo esto a bajos costos; pero pocas veces se consideran los riesgos o implicaciones que pueden suscitar estas nuevas plataformas.

La seguridad digital es un proceso que se basa en la **creación de distintas capas de protección** alrededor de los equipos y la información, de tal forma que se construyan barreras de seguridad exhaustiva.

El primer paso a seguir es **evaluar las amenazas** potenciales y debilidades para diseñar a partir de este conocimiento los planes de acción adecuados según las necesidades particulares, de tal forma que se empleen las herramientas precisas para hacerle frente a los ataques que se puedan suscitar.

Esta guía presenta un conjunto de recomendaciones para un uso seguro de Internet, no pretendemos presentar todas las soluciones posibles para los diferentes problemas que se pueden presentar en el uso de estas tecnologías; sólo queremos fortalecer las capacidades de protección digital de los defensores y organizaciones de derechos humanos, así como ampliar las destrezas en el proceso de identificación de las amenazas en estas plataformas y las acciones inmediatas a llevar a cabo en situaciones concretas.

En primer lugar la responsabilidad de la seguridad digital recae en los usuarios

El tema de la seguridad digital se refiere principalmente a la seguridad de la información que debe ser protegida para evitar que sea robada, dañada, comprometida o restringida, Internet ha ampliado las capacidades de las organizaciones defensoras de derechos humanos a adquirir una voz global ofreciendo oportunidades para acceder y difundir información. Sin embargo, cada vez más los gobiernos restrictivos y empresas desarrollan mecanismos para restringir la información y "hackear" sistemas informáticos para causar daño.

La seguridad digital perfecta casi nunca se alcanza pero es posible **fortalecerla con algunas prácticas sencillas** que si se implementan continuamente mejorarán la protección de la información sensible y se evitará poner en riesgo a las víctimas así como a los defensores que trabajan para ellos.

Algunas preguntas a formularse para elaborar un plan de acción:

• ¿Dónde están almacenados los datos?

Conocer el lugar y/o dispositivos en los cuales se tiene almacenada la información y los archivos, así como las copias de seguridad y respaldo de los archivos.

• ¿Quién conoce su contraseña?

Es importante no revelar la contraseña a ninguna persona porque intrusos podrían acceder a ella y destruir archivos e información sensible.

• ¿Quién puede acceder a su computador?

Conocer las personas que pueden acceder a su computador, y asegurarse que los responsables de esos equipos los apaguen al finalizar la jornada de trabajo o al alejarse por largos períodos de tiempo. Esto permitirá que las contraseñas de BIOS o Windows formen una barrera de protección adicional y al mismo tiempo evita que virus informáticos actúen durante la noche.

• ¿Quién es el remitente de sus mensajes de correo electrónico?

Si al recibir un correo electrónico o algún enlace desconoce al remitente, elimínelo inmediatamente y evite abrirlo porque estos archivos pueden contener virus informáticos que podrían afectar su equipo y destruir su información.

1. **La seguridad digital recae en primer lugar en los usuarios**
2. **Conocimiento mínimo sobre el funcionamiento de los computadores y sus programas**
3. **Ser conscientes de las capacidades y debilidades en materia de seguridad digital**

Las primeras vulneraciones de la seguridad digital se pueden originar a través de correos electrónicos infectados y/o programas maliciosos. En los casos de usurpación de identidad y "hackeo" en Venezuela se detectó que los signos de los ataques tuvieron su origen en:

1- Uso de contraseñas débiles en computadores y servicios de internet

2- Los ataques se inician a través de cuentas de correos electrónicos

3- La ausencia de uso de Anti malware

Por tal razón, es necesario iniciar el proceso de protección digital mediante la **protección de los equipos de trabajo** de los defensores, ante posibles vulneraciones en la seguridad, así como filtraciones a sus sistemas de correo.

Es fundamental:

Usar contraseñas fuertes mediante la combinación de números, letras mayúsculas- minúsculas y caracteres especiales (# ” = @)

Usar un protocolo de seguridad de Wifi WPA2

No usar Wifi abiertas o cibercafés para revisar correos electrónicos

Disponer de dos correos electrónicos personales, para aplicaciones y suscripciones, y otro para compartir con conocidos

1- Proteger tu computadora de software malicioso (malware) y piratas informáticos (hackers)

Es importante garantizar que tu computadora no sea vulnerable a los ataques de hacker ni esté infectada por software malicioso como virus y software espías.

Los virus pueden dañar o infectar tu computadora y tus documentos, incluso los discos externos. Además, pueden tomar control de ella e infectar a otras computadoras.

Por otra parte, los software espías son la clase de software malicioso (malware) que pueden rastrear el trabajo que se realiza en tanto en la computadora como en Internet, enviar esa información a terceros no autorizados, así como registrar las palabras que empleas en el teclado, páginas web que visitas y programas que ejecutas.

Recomendaciones

- Ser cuidadoso al abrir archivos adjuntos en correo electrónico
- Considerar los riesgos al abrir archivos en dispositivos extraíbles
- Deshabilitar la opción “Reproducción Automática” de tu sistema operativo
- Nunca aceptes ni ejecutes programas si vienen de un sitio web que no conoces o en el cual no confías
- Mantenerse alerta cuando se navegue en sitios web
- Instalar antivirus gratuitos y originales en los equipos

2- Crear y mantener contraseñas seguras

La creación de contraseñas seguras, representa un reto para algunas personas porque no solo deben ser fuertes sino también fáciles de recordar, y al mismo tiempo es necesario incorporar números, letras en mayúsculas y minúsculas, y caracteres especiales.

Una contraseña fuerte proporciona la primera, y a veces la única, barrera entre tu información y cualquiera que pudiera leerla, copiarla, modificarla o destruirla sin permiso.

Elementos de una contraseña fuerte

- Debe ser compleja al incluir números, caracteres especiales y letras en mayúsculas y minúsculas
- Debe ser larga, aproximadamente 10 caracteres
- Debe ser práctica para que sea fácil de recordar
- No debe estar relacionada a nivel personal
- Debe mantenerse en secreto
- Cambiar su contraseña cada 3-6 meses

Un recurso útil para recordar las contraseñas

Una solución sencilla para elaborar contraseñas seguras y fáciles de recordar consiste en asociar un tópico de referencia que signifique algo para la persona que lo crea, y transformarlo de tal manera que incluya números y letras, por ejemplo:

- Seleccionar el título de un libro, diremos que es El Principito
- Luego transformaremos el título para incluir números y letras
- Una recomendación sería convertir las letras en números similares (la letra i se parece a un 1, la o a un 0 -cero- la A a un 4, la E en un 3, entre otras)
- Nuestra contraseña final sería **3lpr1nc1p1t0**

Otro mecanismo recomendado es emplear herramientas digitales de gestión de contraseñas, entre ellas, se encuentra Lastpass y KeePass, sistemas que te permiten generar contraseñas aleatorias y complejas para cada aplicación o herramienta que utilices en Internet.

Al utilizar este método es importante crear una contraseña sólida porque será la barrera principal para evitar que intrusos accedan a la caja fuerte con tus claves de acceso a las distintas plataformas digitales.

Lastpass

Es un manejador de contraseñas que permite generar contraseñas aleatorias, compartirlas con terceros y crear notas seguras mediante el uso de sistema cifrado de la información.

Pasos para su uso

- El usuario necesita ingresar a www.lastpass.com
- Descargar el programa e instalarlo
- Seleccionar el idioma de preferencia
- Seguir las instrucciones, en primer lugar le dará la bienvenida a la aplicación y le preguntará si desea instalar los completos para los navegadores (opción útil para uso cotidiano)
- Seleccionar la opción para crear una cuenta en Lastpass
- Colocar el correo electrónico de su preferencia
- Crear una contraseña maestra que será su llave principal para el manejo de sus otras contraseñas, por lo tanto debe ser **suficientemente segura** pues será la primera puerta de entrada a su caja fuerte. Y para finalizar deberá proporcionar algún recordatorio de su contraseña maestra que le será útil en caso de que olvide.

• Aceptar los términos y condiciones para finalizar el proceso de creación de la cuenta.

Uso cotidiano

Una vez instalado Lastpass usted deberá ingresar a cada uno de los servicios y aplicaciones que desea guardar.

En la esquina superior de su navegador se mostrará un botón con el ícono de Lastpass, mediante el cual podrá acceder a su caja fuerte, crear y compartir contraseñas aleatorias, así como gestionar los distintos perfiles de usuarios según el criterio de organización.

3- Cifrar los archivos

Otra barrera de protección para tus archivos y tu información es el cifrado de los archivos, que consiste en hacerlos ilegibles a cualquier persona que no sea su dueño, o se pueden esconder dichos archivos confiando en que el intruso no será capaz de acceder a la información sensible.

Al momento de cifrar los contenidos se ha de considerar que algunas veces implementar esta herramienta puede activar las alarmas de gobiernos represivos, por lo cual se debe ser muy cuidadoso al momento de usarlo.

¿Por qué cifrar archivos?

Fortalece el sistema de seguridad porque la información se encuentra en una especie de caja fuerte, a la cual solo aquellos que tengan la combinación exacta pueden acceder. Una herramienta recomendada es **True Crypt.**

Qué es True Crypt y cómo usarlo

Es un programa libre que mantiene tus archivos en secreto y protegidos mediante contraseña, la cual es asignada por el usuario, y solo mediante ella se puede acceder. Funciona como un caja fuerte, si se pierde la contraseña será imposible acceder a la información.

True Crypt posee niveles de uso según el usuario, que abarca desde principiantes hasta avanzados. En cada una de las categorías de protección ofrece volumen oculto y volumen común; ambos mantendrán confidencial tu información.

El volumen oculto permite esconder tu información importante detrás de otros archivos menos sensibles, incluso si tuvieses que revelar el volumen de True Crypt.

El programa se puede descargar en la página www.truecrypt.org.

4. Destruir datos sensibles

Cuando se borra un archivo en Windows, la información permanece en el disco duro incluso al vaciar la papelera de reciclaje, por lo cual es posible ser recuperada con las herramientas y programas adecuados.

Así para garantizar que la información borrada caiga en las manos equivocadas, es necesario destruir de forma segura y permanente estos archivos con programas como **Eraser**, es un programa de borrado seguro de código abierto.

Eraser permite eliminar permanentemente los archivos, ya sea seleccionando solo el archivo, el contenido de la papelera de reciclaje o borrando todo el contenido no asignado en la unidad.

Otra práctica recomendada es eliminar el historial de navegación y archivos temporales con herramientas como Ccleaner (**www.piriform.com/ccleaner**) que permite borrar el rastro que se produce mientras se visitan diferentes sitios web.

Borrar constantemente el historial de navegación

Eliminar la información sensible en los distintos dispositivos de almacenamientos

Eliminar permanentemente los datos de viejos disco duros antes de regalarlos

Destruir respaldos obsoletos

5- Evadir la censura

Actualmente, gobiernos y empresas han desarrollado software para evitar que los usuarios accedan a ciertos sitios web y servicios de Internet, mediante la aplicación de filtros para bloquear las direcciones IP, elaborando listas negras de dominios, entre otros mecanismos.

Sin embargo, es posible evadir estos mecanismos mediante computadores intermediarias fuera del país, que son conocidas como proxies.

Lo primero a conocer es cómo funciona la conexión a Internet que se realiza típicamente a través del Proveedor de Servicio de Internet (ISP), este le asigna a tu computadora una dirección IP, la cual puede ser utilizada por los servicios de Internet para identificarte y enviarte información. Con la dirección IP es posible identificar la ciudad en la que te encuentres.

Cuando se visualiza una página web, el proceso que ocurre es que le muestras la dirección IP a tu proveedor de Servicio de Internet y le solicitas que se conecte con el Proveedor de servicio de Internet del servidor web. En los países con censura en Internet, primero se consultará si el sitio web al que deseas acceder no se encuentra en la lista de sitios web prohibidos antes de decidir si te deja acceder o no.

Este bloqueo puede ser evadido mediante servidores proxies seguros, que proporcionan un desvío para buscar las páginas web solicitadas y enviártelas; esto es posible porque provienen de un país en el cual no se filtra el Internet. Entonces, para tu Proveedor de Servicio de Internet aparecerás comunicándote con una computadora desconocida en algún lugar de Internet.

El programa recomendado para lograr la evasión y proporcionar anonimato es **Tor** (https://www.torproject.org/), el que primero deberás instalar y luego, cada vez que te conectes a su red, seleccionarás una ruta aleatoria a través de sus proxies seguros. Con esto se garantiza que ni tu Proveedor de Servicio de Internet ni los mismos proxies conozcan tu dirección IP o la ubicación de los servicios de Internet que solicitas.

Recomendaciones finales

- Activar la clave de verificación de dos pasos de plataformas como gmail, dropbox, facebook
- Usar VoIP (Voz sobre Protocolo de Internet) como Skype
- Realizar respaldos continuos de la información
- Emplear códigos de bloqueo para el teléfono móvil y nunca dejarlo sin atención
- Eliminar el historial y los archivos temporales con programas como ccleaner
- Descargar los programas desde los sitios web de sus creadores

Verificación de dos pasos

Es una segunda capa de protección de la información que posees en los servicios de Internet (Gmail, Facebook y Dropbox, por mencionar algunos) compuesta por dos factores claves: información que conoces(contraseña) e información que tienes en tu poder (código de verificación en tu celular).

Este nuevo paso garantiza que si terceras personas no autorizadas desean ingresar a tu cuenta de correo electrónico, necesitarán l**a contraseña y además un código** que te proporcionará el servicio de Internet de manera aleatoria en tu celular, mediante una llamada, sms o tarjeta de códigos adicionales.

Referencias

- Security in box. Tactical Technology Collective and Front Line. Consultado en: https://security.ngoinabox.org/es
- Seguridad Digital y privacidad digital para los defensores de Derechos Humanos. Front Line. Consultado en http://www.frontlinedefenders.org/es/digital-security
- Buenas prácticas para la distribución y publicación de información sensible en Internet. Rafael Nuñez. Consultado en http://www.slideshare.net/espaciopublico/buenas-prcticas-para-la-distribucin-y-publicacin-de-informacin-sensible?from=ss_embed

espacio público

A. C. Espacio Público
www.espaciopublico.org
Espacio Público
@espaciopublico