¿Te interesa que nadie pueda espiar tu correo electrónico?

Por Andrea Cárdenas

El uso de contraseñas complejas para acceder a tu correo electrónico o actualizarlas con cierta frecuencia ya no es suficiente para proteger tu información. En los últimos meses han salido a la luz casos de hackeos a las cuentas de periodistas.

Quinto Elemento Lab consultó a expertos en seguridad cibernética para periodistas sobre medidas para evitar ataques de los hackers y sistemas de espionaje que buscan intervenir las comunicaciones y tener acceso a información sensible que manejan los reporteros.

Estas son las recomendaciones de Paul Aguilar de SocialTic y las sugerencias vertidas en un manual de la organización Artículo 19.

Medidas de seguridad:

1. **Activa en dos minutos la "verificación en dos pasos".** Con este servicio disponible para gmail, hotmail y yahoo protegerás tu cuenta utilizando dos elementos: una contraseña y tu número telefónico. Incluso si un hacker consigue la contraseña, necesitaría además tu teléfono o tu llave de seguridad para acceder a tu cuenta de correo electrónico.

   Cada vez que inicias sesión debes introducir tu contraseña y en automático se enviará un código a tu teléfono mediante un mensaje o llamada de voz para que puedas ingresar a tu cuenta. Esta herramienta además te permitirá detectar si alguien intenta ingresar a tu correo y te enviará una notificación con tu código de seguridad al celular. El intruso nunca tendrá acceso al código aunque conozca tu usuario y contraseña.
   Haz clic aquí para activarla:
   https://www.google.com/landing/2step/?utm_source=pp&hl=es_419

2. **Borra tu rastro.** Evita iniciar sesión en un equipo que no sea el tuyo, o en una computadora pública, ya que corres el riesgo de que algún programa implantado registre la actividad de tu teclado y tu contraseña cuando ingresas a tu cuenta. Si no tienes otra alternativa la recomendación es ingresar a tu correo desde una ventana de incógnito para que tu inicio de sesión no se registre en el historial de la computadora.

Al navegar en privado lo que haces es borrar tu huella para que otros usuarios que utilicen el dispositivo no vean tu actividad. Si utilizas esta opción que ofrecen diferentes navegadores, al salir del modo incógnito se borrará tu historial de navegación, las cookies, los datos de sitios web o la información que hayas introducido al ingresar a tu cuenta. Solo debes tener cuidado con los archivos que descargues ya que seguirán en la carpeta "Descargas" aún después de salir del modo incógnito. Para ingresar a este modo en Chrome, haz clic en Más  Nueva ventana de incógnito, en la parte superior derecha de la página. Entonces se abrirá una nueva ventana. En la esquina superior, busca el icono de incógnito  para confirmar que estés en un portal de navegación segura.

3. **Cuidado con las redes abiertas.** Al conectarte a una red WiFi abierta en salas de prensa, restaurantes, aeropuertos o espacios públicos, tu información queda expuesta y una persona con experiencia en hackeo puede acceder a todo lo que haces: puede revisar tus correos, tus mensajes o incluso robar tus contraseñas porque tus datos viajan sin protección y pueden ser detectados fácilmente por el atacante, quien puede capturar tus contraseñas, robar dinero de tu cuenta bancaria, infectar tu equipo o redirigirte a páginas fraudulentas para robar tu información.
   Si ingresas a una red abierta, los expertos recomiendan usar una red privada virtual para que nadie pueda acceder a la información que compartes.
   Hay una serie de programas que puedes instalar en tu computadora, que garantizarán que toda tu información viaje encapsulada, y que nadie pueda tener acceso a ella durante su viaje por la red.
   Este tipo de programas también te permiten escapar de las restricciones regionales de contenidos y sitios o enviar tu información desde cualquier lugar del mundo.
   Existen algunos servicios como:
   - HotSpotShield
   - YourFreedom
   - PIA VPN
   - Tunnel Bear

4. **Asegúrate antes de abrir un correo**. Analiza con detenimiento las solicitudes de información personal que recibas en tu correo y los archivos adjuntos de personas desconocidas. Si tienes alguna duda sobre la dirección del remitente es mejor que investigues su procedencia y verifiques su identidad, ya que alguien podría montar un portal falso para robar tus datos personales o enviarte archivos adjuntos que buscan infectar tu equipo y tomar el control de tus cuentas de correo. Es recomendable analizar con un antivirus los correos sobre los que tengas alguna duda. Haz caso de las alertas de tu antivirus antes de que sea demasiado tarde.

5. **Diversifica tus cuentas.** Utiliza diferentes direcciones de correo electrónico para tus actividades. Puedes manejar una cuenta para tus actividades personales y otra para tus tareas profesionales para no poner en riesgo toda tu información en caso de que accedan a una de tus cuentas.

6. **Cierra tu sesión.** No olvides cerrar sesión después de haber consultado tu correo y así evitar que alguien tenga la tentación de revisar tu información si tienen acceso a tu equipo. Cuando manejas información sensible, la recomendación es cerrar sesión cada que sales de tu cuenta. Si usas Gmail, en la bandeja de entrada, ve hacia abajo. En la esquina inferior de la página, a la derecha, haz clic en la liga "Detalles" y verás toda la actividad de tu cuenta. En esta sección puedes ver tu historial de inicios de sesión con las fechas y horas a las que se utilizó tu cuenta. También puedes ver las direcciones IP que se han usado para acceder a tu correo. Ahí podrás cerrar la sesión en cualquiera de los dispositivos. Esta herramienta te ayudará a detectar si alguien ingresó a tu correo. En el apartado "datos de la sesión simultánea" podrás ver si tienes una sesión abierta en otro dispositivo, navegador o ubicación, mientras que en "tipos de acceso" se muestra el navegador, dispositivo o el servicio de correo con el que accediste a tu cuenta. La recomendación es realizar esta verificación de manera periódica y cerrar las sesiones iniciadas que no reconozcas o que ya no estés utilizando.

7. **No entres en automático**. Otra sugerencia es cambiar la configuración de tu cuenta para que tu servidor no inicie sesión en automático. En la parte superior derecha, haz clic en Perfil y Contraseñas para activar o desactivar la opción "preguntar si quiero guardar contraseñas".

8. **Revisa las alertas.** Para revisar las notificaciones de actividad sospechosa en tu cuenta, como accesos desde dispositivos y ubicaciones desconocidos, debes ingresar a la sección "eventos recientes de seguridad", en donde podrás ver una lista de alertas de los últimos 28 días sobre los accesos bloqueados, los cambios de contraseña o si agregaste un número de teléfono a la cuenta. Comprueba la lista para confirmar que reconoces todas las alertas y notificaciones enlistadas.

9. **No utilices la misma contraseña para diferentes páginas o servicios**. Es como usar la misma llave para diferentes puertas y si alguien más tiene acceso a tu contraseña intentará usarla en tus otras cuentas de correo o redes sociales. Además, las diferentes filtraciones masivas de contraseñas podrían haber expuesto ya tu contraseña y con ello ponerte en grave riesgo. Puedes consultar de manera segura si alguna de tus contraseñas ha sido expuesta en internet en: https://haveibeenpwned.com

10. **Cambia tus contraseñas de manera periódica.** Es recomendable que lo hagas cada dos semanas o una vez al mes dependiendo de la información que manejes. Es deseable incluir números y símbolos como * o # y utilizar palabras inconexas entre sí o palabras en distintos idiomas. No utilices nombres de familiares, datos personales, fechas de cumpleaños o claves comunes como "1234…" que alguien más pueda adivinar fácilmente. Una contraseña segura debe ser larga, mínimo de 12 caracteres.

    Utiliza un gestor de contraseñas. Nunca anotes tus contraseñas en una libreta, en una nota de celular o en un archivo de computadora. Para generar y almacenar contraseñas seguras considera utilizar un gestor de contraseñas: Keepass, Dashlane, IPassword,

Lastpass son algunos servicios. Este tipo de programas cifran el acceso a tus contraseñas y te permiten acceder a ellas desde tu celular, a través de una USB o por medio de dropbox o Google drive. Además, puedes copiar y pegar los accesos a tus cuentas sin necesidad de escribirlos y te ofrecen mecanismos para que el archivo encriptado no esté accesible para otro tipo de programas que puedas tener instalados. Los especialistas recomiendan utilizar solo los programas que puedas instalar en tu computadora para cifrar el archivo donde almacenarás tus claves ya que solo tú podrás acceder a ese archivo con una contraseña. Los gestores de contraseña que ofrecen Google y Mac y que se encuentran en la nube, no son los más recomendables pues tu información estará resguardada en el servidor de un tercero. Y aunque no deberían acceder a tus datos, no hay seguridad de que sea así. Si quieres saber más sobre la utilidad y seguridad de estas empresas te dejamos este link: https://www.wired.com/story/password-manager-autofill-ad-tech-privacy/

11. **Cifra tus correos**. Existen programas para cifrar el contenido de tus correos (textos, documentos adjuntos, bases de datos, presentaciones) antes de enviarlos por internet. Solo debes tener cuidado con el nombre del asunto y de los archivos que adjuntes pues es lo único que no se cifrará. Para evitar que un tercero fisgonee en tus comunicaciones puedes utilizar servicios como:
    - https://protonmail.com/
    - https://tutanota.com/es/
    - https://www.mailvelope.com/en

    Haz clic para ver el manual de mailvelope que nos compartió el Consorcio Internacional de Periodistas de Investigación (ICIJ). Este programa es el que utilizan los periodistas que colaboran con esta organización para encriptar sus comunicaciones.

12. **Recupera tu cuenta**. Si ya te hackearon lo primero que debes hacer es mantener la calma y contactar al proveedor de tu correo para recuperar tu cuenta y restablecer tu contraseña. Tu proveedor te pedirá un número telefónico o un correo alternativo para enviarte un enlace de recuperación de cuenta. Solo deberás responder unas preguntas para que verifiquen que efectivamente eres el titular de la cuenta. Para evitar que tus contactos corran con la misma suerte, no olvides poner sobre aviso a tus colaboradores más cercanos y alertarlos para que no abran ningún correo de tus cuentas hasta que logres solucionar el problema de seguridad.