



El Boletín Mensual de Concientización en Seguridad para ti

Limpieza de primavera digital en siete sencillos pasos

Resumen

Frecuentemente escuchamos el término "limpieza de primavera", la época del año en la que revisamos nuestras pertenencias y organizamos nuestra casa y nuestra vida en preparación para el próximo verano. Este también es el momento perfecto para hacer una revisión anual de tu vida digital. Los siguientes siete sencillos pasos, realizados una vez al año, ayudarán bastante a garantizar que puedas aprovechar al máximo la tecnología de forma segura.

CUENTAS: Revisa cada una de tus cuentas. El uso de una contraseña larga y única para cada cuenta garantiza que, si una cuenta se ve comprometida, tus otras aún están seguras. ¿No recuerdas todas tus contraseñas? No te preocupes, nosotros tampoco. Te recomendamos que utilices un gestor de contraseñas para almacenar de forma segura todas tus contraseñas y hacer tu vida mucho más simple y segura. Habilita la autenticación multifactor (MFA, por sus siglas en inglés) cuando sea posible, especialmente para tu correo electrónico personal o cuentas financieras. Este es el paso más importante que puedes tomar para asegurar cualquier cuenta en línea. Si tienes cuentas en línea a las que no has accedido en más de un año, podría ser el momento para simplemente eliminarlas.

PROGRAMAS: Mantener tus dispositivos y software actualizados garantiza que tengan instaladas las funciones de seguridad más recientes y que se corrijan las vulnerabilidades conocidas. La forma más sencilla de hacer esto es asegurarse de tener habilitadas las actualizaciones automáticas en todas tus computadoras, dispositivos móviles e incluso dispositivos inteligentes del hogar. Además, elimina cualquier programa o aplicación que no utilices en tus dispositivos móviles y computadoras. Algunas aplicaciones requieren grandes cantidades de almacenamiento, pueden introducir nuevas vulnerabilidades e incluso ralentizar las cosas. Mientras menos aplicaciones tengas, más seguro serán tus sistemas e información. Muchos dispositivos te muestran cuánto tiempo ha pasado desde que usaste una aplicación. Si ha pasado un año desde la última vez que usaste la aplicación, es probable que ya no la necesites.

FINANZAS: verifica que tus cuentas bancarias, cuentas de tarjetas de crédito, inversiones y cuentas de ahorro para el retiro estén configuradas para alertarte cada vez que se realiza una transacción, especialmente para inicios de sesión inusuales, compras grandes o transferencias de dinero. Esto hará que siempre se te notifique cuando se produzca una transacción financiera y puedas detectar cualquier fraude o actividad no autorizada de inmediato. Cuanto antes identifiques la actividad fraudulenta, podrás detenerla y será más probable que puedas recuperar tu dinero. Dependiendo del país en el que vives, un paso adicional que puedes tomar es implementar un congelamiento de crédito, que puede ser una de las formas más efectivas de proteger tu identidad.

ELIMINACIÓN DE DISPOSITIVOS: Con el tiempo, es posible que te encuentres recolectando dispositivos antiguos que ya no necesitas, tal vez un teléfono inteligente antiguo o un dispositivo inteligente para el hogar. Si te deshaces de alguno de estos dispositivos, primero borra cualquier información personal almacenada en ellos. La mayoría de los dispositivos tienen una función simple de borrado que elimina de forma segura toda la información personal (o restablece los valores predeterminados de fábrica) antes de desechar el dispositivo.

RESPALDOS : No importa qué tan seguro o protegido estés, en algún momento probablemente necesitarás respaldos para recuperar información importante o migrar la información a un nuevo dispositivo. Configura tus dispositivos para que realicen una copia de seguridad automática en la nube. Crear y programar copias de seguridad automáticas te permite recuperar tu información más importante.

CONTROL PARENTAL: Si eres padre o tutor, este es un buen momento para revisar cualquier configuración de control parental que tengas para los niños. A medida que los niños crezcan, lo más probable es que necesites actualizar la configuración de estos controles.

REDES SOCIALES: Revisa la configuración de privacidad en tus cuentas de redes sociales, estas son una mina de oro de información personal. Revisa tus cuentas para verificar que no estés compartiendo información confidencial, como tu cumpleaños, número de teléfono, domicilio, información bancaria o ubicación geográfica en fotos personales.

Dedicar solo un par de horas al año a seguir estos pasos contribuirá en gran medida a protegerte a ti, tus dispositivos y tu información.

Editor invitado

Ritu Gill ([@OSINTtechniques](https://twitter.com/OSINTtechniques)) es instructora del SANS en desarrollo y analista de inteligencia que se especializa en inteligencia de fuentes abiertas (OSINT). Más información sobre Ritu aquí: <https://www.sans.org/profiles/ritu-gill> y aquí <https://www.osinttechniques.com>.



Recursos

Gestores de contraseñas: <https://www.sans.org/newsletters/ouch/password-managers/>

El poder de actualizar: <https://www.sans.org/security-awareness-training/resources/power-updating>

Desechando tus dispositivos móviles: <https://www.sans.org/newsletters/ouch/disposing-mobile-devices/>

¿Tienes respaldos?: <https://www.sans.org/newsletters/ouch/backups/>

Protegiendo a los niños: <https://www.sans.org/newsletters/ouch/online-security-kids>

Traducido para la comunidad por: Cécica Martínez Aponte e Iván Galindo, UNAM-CERT

OUCH! Es publicado por SANS Security Awareness y es distribuido bajo la licencia [Creative Commons BY-NC-ND 4.0 license](https://creativecommons.org/licenses/by-nc-nd/4.0/). Puedes distribuir y compartir este boletín, siempre y cuando no lo vendas o modifiques. Consejo editorial: Walter Scrivens, Phil Hoffman, Alan Waggoner, Leslie Ridout, Princess Young.