SEA CIBERNÉTICAMENTE INTELIGENTE
#CyberMonth

MES DE CONCIENTIZACIÓN SOBRE SEGURIDAD CIBERNÉTICA DE 2021: PONGA DE SU PARTE. #BECYBERSMART

CÓMO PROTEGER SU HOGAR DIGITAL

Muchos de los dispositivos en nuestras casas—incluyendo los termostatos, cerraduras de puertas, cafeteras y alarmas de incendios—ahora están conectados a Internet. Esto nos permite controlar los dispositivos en nuestros teléfonos inteligentes, lo cual nos puede ahorrar tiempo y dinero, además de proporcionar conveniencia y seguridad adicional. Estos avances en la tecnología son innovadoras y llamativas, pero también representan un nuevo conjunto de riesgos de seguridad. #BeCyberSmart para conectarse con confianza y proteger su hogar digital.

CONSEJOS SENCILLOS

- **Asegure su red Wi-Fi.** El enrutador inalámbrico de su hogar es la entrada principal a través de la cual los delincuentes cibernéticos podrían acceder a sus dispositivos conectados. Asegure su Wi-Fi y sus dispositivos digitales al cambiar la contraseña y el usuario predeterminados. Para más información sobre cómo proteger la red de su hogar, visite la página de CISA sobre Cómo asegurar las redes inalámbricas.
- **Duplique la protección de sus credenciales.** Habilite la autenticación por múltiples factores (MFA, por sus siglas en inglés) para asegurar que la única persona con acceso a sus cuentas sea usted mismo. Úsela para su correo electrónico, su banco, sus redes sociales y todo otro servicio que requiere que inicie sesión. Si MFA es una opción, habilítela con un dispositivo móvil fiable, tal como su teléfono inteligente, una aplicación de autenticación o un token seguro—un dispositivo físico pequeño que puede llevar en su llavero. Para más información, lea la Guía a la Autenticación por Múltiples Factores (MFA, por sus siglas en inglés).
- **Si se conecta, debe proteger.** Ya sea su computadora, teléfono inteligente, dispositivo de juegos u otros dispositivos de las redes, la mejor defensa es mantenerse al día, actualizando a las últimas versiones de los programas se seguridad, los navegadores web y los sistemas operativos. Si tiene la opción de habilitar actualizaciones automáticas para defender contra los últimos riesgos, habilítelas. Y, si introduce algo en su dispositivo, tal como una unidad flash o un disco duro externo, asegure que el software de seguridad de su dispositivo lo analice para detectar virus y programas maliciosos. Por último, proteja sus dispositivos con software antivirus y asegúrese de respaldar periódicamente todos los datos que no se pueden remplazar, tales como sus fotos o documentos personales.
- **Monitoree sus aplicaciones.** La mayoría de los electrodomésticos, juguetes y dispositivos conectados son apoyados por una aplicación móvil. Su dispositivo móvil podría estar lleno de aplicaciones sospechosas que operan al fondo o usan permisos automáticos que usted nunca se dio cuenta que había aprobado—para recolectar su información personal sin su conocimiento mientras ponen en riesgo su identidad y su privacidad. Verifique los permisos de sus aplicaciones y use la "regla del menor privilegio" para borrar lo que no necesita y lo que ya no usa. Aprenda a decir "no" a las solicitudes de privilegios que no tienen sentido. Solo descargue aplicaciones de proveedores y fuentes de confianza.

- **Nunca haga clic para decir de todo.** Limite la información que publique en las redes sociales—desde direcciones personales hasta su lugar favorito para comprar café. Muchas personas no se dan cuenta que estos detalles que parecen aleatorios representan todo lo que los delincuentes necesitan para enfocarse en usted, sus seres queridos y sus pertenencias personales—por Internet y en el mundo real. Mantenga confidenciales sus números de Seguro Social, números de cuentas y contraseñas, también como toda información específica sobre usted, tal como su nombre completo, su dirección, su cumpleaños y sus planes de vacaciones. Desactive los servicios de ubicación que permitan que cualquier persona pueda ver donde usted se encuentra—y donde no se encuentra—en cualquier momento. Para más información, lea la Hoja de consejos sobre la seguridad cibernética en redes sociales.
- **Tenga cuidado al compartir archivos.** Debe desactivar la función de compartir archivos entre dispositivos cuando no la necesita. Siempre debe optar por permitir solamente el intercambio de archivos en redes de su hogar y de su trabajo, nunca en redes públicas. Podría ser buena idea pensar en crear un directorio dedicado para compartir archivos y restringir el acceso a todo otro directorio. Además, debe proteger con contraseña cada archivo que comparte.
- **Verifique las opciones de seguridad inalámbrica de su proveedor de Internet y del fabricante de su enrutador.** Es posible que su proveedor de servicio de Internet y el fabricante de su enrutador proporcionen información o recursos para ayudarle a asegurar su red inalámbrica. Consulte el área de apoyo al cliente de sus páginas web para obtener sugerencias o indicaciones específicas.
- **Conéctese con una Red Privada Virtual (VPN, por sus siglas en inglés).** Muchas compañías y organizaciones tienen VPN. Las VPN permiten que los empleados se conecten de manera segura a su red cuando estén fuera de la oficina. Las VPN encriptan las conexiones en los extremos de envío y recepción y bloquean el tráfico que no esté cifrado de manera apropiada. Si hay una VPN disponible para usted, asegúrese de iniciar sesión en la VPN cada vez que necesita usar un punto de acceso inalámbrico público.
- **Restrinja el acceso.** Solo debe permitir que los usuarios autorizados accedan a su red. Cada equipo que se conecta a una red tiene una dirección de control de acceso a medios (MAC, por sus siglas en inglés). Para restringir el acceso a su red, puede filtrar estas direcciones MAC. Para información específica sobre cómo habilitar estas funciones, consulte la documentación del usuario. También puede utilizar la cuenta del "invitado", una función común en muchos enrutadores inalámbricos. Esta función le permite dar acceso inalámbrico a los invitados en un canal inalámbrico distinto con una contraseña diferente, mientras mantiene la privacidad de sus credenciales principales.

COMUNÍQUESE CON EL EQUIPO DEL MES DE CONCIENTIZACIÓN SOBRE SEGURIDAD CIBERNÉTICA DE CISA

Muchas gracias por su apoyo y compromiso continuos con el Mes de Concientización sobre Seguridad Cibernética y por ayudar a todos los estadounidenses a mantenerse seguros en Internet. Para aprender más, envíe un mensaje por correo electrónico a nuestro equipo en CyberAwareness@cisa.dhs.gov, o visite www.cisa.gov/cybersecurity-awareness-month o staysafeonline.org/cybersecurity-awareness-month/.