SEA CIBERNÉTICAMENTE INTELIGENTE
#CyberMonth

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

PRIVACIDAD EN INTERNET

El Internet toca casi todos los aspectos de nuestras vidas diarias. Podemos hacer compras, realizar transacciones bancarias, conectarnos con familia y amigos y administrar nuestros registros médicos, todo por Internet. Estas actividades exigen que proporcione información personalmente identificable (PII, por sus siglas en inglés), tal como su nombre, fecha de nacimiento, números de cuentas, contraseñas e información de ubicación. #BeCyberSmart cuando comparte su información personal por Internet para reducir el riesgo de ser víctima de delitos cibernéticos.

¿SABÍA USTED?

- Un 72% de los estadounidenses creen que la mayoría de lo que hacen por Internet es rastreada por anunciantes, empresas de tecnología y otras compañías.[1]
- Más de la mitad de los estadounidenses (52%) dicen que han decidido no usar algún producto o servicio porque estaban preocupados por la cantidad de información personal que recolectaba de ellos.[1]
- Los costos por filtraciones de datos ascendieron de USD 3.86 millones a USD 4.24 millones en 2021.[2]
- Credenciales comprometidas, tales como las contraseñas, eran responsables del 20% de las filtraciones con un costo promedio por filtración de USD 4.37 millones..[2]

CONSEJOS SENCILLOS

- **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).
- **Altere su protocolo para sus contraseñas.** Utilice la contraseña o frase de contraseña más larga que se permita. Sea creativo y adapte su contraseña estándar para páginas diferentes, ya que esto puede evitar que los delincuentes cibernéticos obtengan acceso a estas cuentas y proteger a usted en caso de una filtración de datos. Use administradores de contraseñas para generar y recordar distintas contraseñas complejas para cada una de sus cuentas. Para más información, lea la Hoja de consejos sobre cómo crear una contraseña..
- **Manténgase al día.** Mantenga su software actualizado a la última versión disponible. Mantenga sus configuraciones de seguridad para que protejan su información, activando las actualizaciones automáticas para no tener que pensar en ellas y configure su software de seguridad para que realice análisis regulares.
- **Si lo conecta, protéjalo.** Ya sea su computadora, teléfono inteligente, dispositivo de juegos u otros dispositivos de las redes, la mejora defensa contra los virus y los programas maliciosos es la actualización a las últimas versiones de los programas se seguridad, los navegadores web y los sistemas operativos. Inscríbase para

actualizaciones automáticas, si puede, y proteja sus dispositivos con software antivirus. Para más información, lea la Hoja de consejos sobre phishing.

- **Juegue a hacerse el difícil con extraños.** Los delincuentes cibernéticos utilizan tácticas de phishing para tratar de engañar a sus víctimas. Si no está seguro quién le ha enviado un correo electrónico—incluso si los detalles parecen correctos—o si el correo parece que podría ser un intento de phishing, no responda y no haga clic en los enlaces o los adjuntos en el correo electrónico. Cuando esté disponible, utilice la opción de "spam" o "bloquear" para que no reciba mensajes futuros de un remitente específico.
- **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.
- **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.
- **Manténgase protegido mientras está conectado.** Antes de conectar en cualquier punto de acceso inalámbrico público—tal como en un aeropuerto, hotel o cafetería—asegúrese de confirmar el nombre de la red y los procedimientos precisos para iniciar sesión con el personal apropiado para asegurar que la red sea legítima. Si usa un punto de acceso público no asegurado, practique la buena higiene de Internet al evitar actividades sensibles (por ejemplo, la banca) que requieren contraseñas o tarjetas de crédito. Su punto de acceso personal suele ser una alternativa más segura que el Wi-Fi gratis. Use solamente sitios que empiezan con "https://" cuando hace compras o actividades bancarias por Internet.

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/.

RECURSOS

1. Auxier, Brooke, “How Americans see digital privacy issues amid the COVID-19 outbreak.” Pew Research Center: Fact Tank. 4 de mayo de 2020. https://www.pewresearch.org/fact-tank/2020/05/04/how-americans-see-digital-privacy-issues-amid-the-covid-19-outbreak/
2. IMB, “Cost of a Data Breach Report 2021.” IMB Security. Julio de 2021. https://www.ibm.com/security/data-breach