# SEA CIBERNÉTICAMENTE INTELIGENTE
#CyberMonth

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

## ROBO DE IDENTIDAD Y ESTAFAS EN INTERNET

La tecnología actual nos permite conectar en todas partes del mundo, para realizar transacciones bancarias o hacer compras en Internet, y para controlar nuestros televisores, hogares y automóviles desde nuestros teléfonos inteligentes. Esta conveniencia adicional viene acompañada de un riesgo aumentado de robo de identidad y estafas en Internet. #BeCyberSmart en Internet—en casa, en la escuela, en el trabajo, en los dispositivos móviles y sobre la marcha.

## ¿SABÍA USTED?

- El costo promedio de una filtración de datos para una compañía de los EE. UU. en 2020 era $8.84 millones[1]. Esa cifra es un aumento sobre la cifra de 2019 de $8.64 millones.
- 7-10% de la población de los EE. UU. son víctimas del fraude de identidad cada año, y 21% de ellos experimentan múltiples incidentes de fraude de identidad[2].
- En 2020, 47% de las personas que viven en los EE. UU. experimentaron el robo de identidad[3].

## ESTAFAS COMÚNES EN INTERNET

A medida que la tecnología evoluciona, los delincuentes cibernéticos usarán técnicas más sofisticadas para explotar los sistemas, las cuentas y los dispositivos para robar su identidad, su información personal y su dinero. Para protegerse contra las amenazas en Internet, tiene que saber lo que debe estar buscando. Algunas de las estafas más comunes en Internet incluyen las siguientes:

- **ESTAFAS DE COVID-19** vienen en la forma de correos electrónicos con adjuntos maliciosos o enlaces a páginas web fraudulentas para engañar a sus víctimas para que divulguen su información confidencial o hagan donativas a organizaciones benéficas o causas fraudulentas. Tenga cuidado con todo correo electrónico que tenga un asunto, adjunto o enlace relacionado con COVID-19 y esté atento para las súplicas en redes sociales, los mensajes de texto y las llamadas telefónicas relacionadas con COVID-19.
- **ESTAFAS DE IMPOSTOR** ocurren cuando usted recibe un correo electrónico o una llamada de una persona que dice ser un funcionario del gobierno, un miembro de su familia o un amigo y solicita su información personal o financiera. Por ejemplo, un impostor podría contactar a usted desde la Administración del Seguro Social para informarle que su número de Seguro Social (SSN, por sus siglas en inglés) ha sido suspendido, esperando que usted le divulgue su SSN o le pague para reactivarlo.
- **ESTAFAS DE PAGOS ECONÓMICOS POR COVID-19** tienen como blanco los pagos de estímulo de los estadounidenses. CISA recomienda que todos los estadounidenses estén atentos contra el fraude delictivo relacionado con pagos de impacto económico por COVID-19—en especial el fraude que usa señuelos de coronavirus para robar información personal y financiera, también como los pagos de impacto económico mismos—y contra los adversarios que tratan de interrumpir los esfuerzos de los pagos.

## 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.

- **ALTERE SU PROTOCOLO PARA CONTRASEÑAS.** Según la guía del Instituto Nacional de Estándares y Tecnología (NIST, por sus siglas en inglés), usted debe pensar en usar la contraseña o frase de contraseña más larga que se permite. 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.

## PROTÉJASE CONTRA EL FRAUDE POR INTERNET

**MANTÉNGASE PROTEGIDO MIENTRAS ESTÁ CONECTADO:** El punto clave es que siempre que usted esté conectado al Internet, está vulnerable. Si los dispositivos en su red estuvieran comprometidos por cualquier razón, o si los piratas informáticos penetraran un cortafuegos cifrado, alguien podría estar espiándolo—incluso en su propio hogar con Wi-Fi cifrado.

- Practique la navegación web segura donde sea que se encuentre al verificar que el ícono del "candado verde" esté en la barra de su navegador—esto significa que la conexión es segura.
- Cuando se encuentre en el "lejano oeste de Wi-Fi", evite el acceso gratuito a Internet que no esté cifrado.
- 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.
- No divulgue a fuentes desconocidas su información personalmente identificable, tal como el número de su cuenta bancaria, su SSN o su fecha de nacimiento.
- Ingrese las direcciones URL directamente en la barra de direcciones en lugar de hacer clic en los enlaces o cortar y pegar del correo electrónico.

## RECURSOS DISPONIBLES PARA USTED

Si se da cuenta que ha sido víctima de un delito cibernético, notifique inmediatamente a las autoridades para hacer una denuncia. Conserve y registre todas las pruebas del incidente y su presunta fuente. La lista a continuación describe las organizaciones gubernamentales donde puede hacer una denuncia si ha sido víctima de un delito cibernético.

- **FTC.gov**: El recurso gratuito e integral de la FTC, www.identitytheft.gov/ puede ayudarle a denunciar y recuperarse del robo de identidad. Denuncie el fraude a la FTC en ftc.gov/OnGuardOnline o www.ftccomplaintassistant.gov.
- **US-CERT.gov**: Denuncie vulnerabilidades de computadoras o redes a US-CERT a través de su línea directa: 1-888-282-0870 o en us-cert.cisa.gov. Reenvíe correos electrónicos o páginas web de phishing a US-CERT phishing-report@us-cert.gov.
- **IC3.gov**: Si ha sido víctima de la delincuencia en Internet, haga una denuncia con el Centro de Denuncias de Delitos en Internet (IC3) en www.IC3.gov.
- **SSA.gov**: Si cree que alguien está usando su SSN, comuníquese con la línea directa sobre fraude de la Administración del Seguro Social llamando al 1-800-269-0271.

## 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 http://www.cisa.gov/cybersecurity-awareness-month o staysafeonline.org/cybersecurity-awareness-month/.

## RECURSOS


1. Brook, Chris. (18 de agosto de 2020). *What Does a Data Breach Cost in 2020?* Digital Guardian. https://digitalguardian.com/blog/what-does-data-breach-cost-2020
2. Ricks, A, Irvin-Erickson, Y, PhD (2021). *Research Brief: Identity Theft and Fraud.* Center for Victim Research. https://ncvc.dspacedirect.org/bitstream/item/1228/CVR Research Syntheses_Identity Theft and Fraud_Brief.pdf
3. GIACT. (2021). *U.S. Identity Theft: The Stark Reality*. GIACT Systems, LLC.https://www.giact.com/aite-report-us-identity-theft-the-stark-reality/