

KIT DE HERRAMIENTAS PARA EL MES DE CONCIENTIZACIÓN SOBRE SEGURIDAD CIBERNÉTICA DE 2021

Mensajes claves, artículos, redes sociales y más para promover el Mes de Concientización sobre Seguridad Cibernética de 2021.



ÍNDICE

Bienvenidos al Mes de Concientización sobre Seguridad Cibernética de 2021 _____	3
Temas y mensajes claves para octubre de 2021 _____	3
Tema abarcador de 2021 _____	3
Mensajes claves de 2021 _____	3
Cómo involucrar a otros _____	4
Ideas para involucrar a otros _____	4
Consejos principales para compartir durante el Mes de Concientización sobre Seguridad Cibernética _____	4
Recursos de seguridad cibernética _____	5
Canales de comunicaciones _____	6
Ejemplo de un calendario de comunicaciones _____	6
Comunicaciones en las redes sociales _____	7
Ejemplo de una entrada para su blog _____	11
Ejemplo de un correo electrónico a clientes y al personal _____	12
Ejemplo de un correo electrónico a los clientes: _____	12
Ejemplo de un correo electrónico al personal: _____	13

BE CYBER SMART

#CyberMonth



BIENVENIDOS AL MES DE CONCIENTIZACIÓN SOBRE SEGURIDAD CIBERNÉTICA DE 2021

El Mes de Concienciación sobre Seguridad Cibernética, celebrado cada octubre, es un esfuerzo colaborativo entre el gobierno y la industria para asegurar que cada estadounidense cuente con los recursos necesarios para mantenerse seguro en Internet y aumentar la resistencia de la Nación contra amenazas cibernéticas.

La Agencia de Seguridad Cibernética y Seguridad de la Infraestructura (CISA, por sus siglas en inglés) y la Alianza Nacional de Seguridad Cibernética (NCSA, por sus siglas en inglés) copresiden el Mes de Concienciación sobre Seguridad Cibernética.

Muchas gracias por participar en el Mes de Concienciación sobre Seguridad Cibernética. Para asistir en sus esfuerzos y su participación, este documento incluye una amplia gama de recursos para usted y su organización, independiente de su tamaño o industria, para poder involucrar a otros y promocionar el tema principal y los mensajes críticos desde ahora hasta el fin de octubre.

TEMAS Y MENSAJES CLAVES PARA OCTUBRE DE 2021

Le pedimos que utilice el tema abarcador del Mes de Concienciación sobre Seguridad Cibernética en sus propias iniciativas en octubre. Este año, en el marco del tema de "Ponga de su parte. #BeCyberSmart.", la campaña hará hincapié en el papel que cada individuo juega en la seguridad en Internet y enfatizará la importancia de tomar medidas proactivas para aumentar la seguridad cibernética en casa y en el trabajo.

TEMA ABARCADOR DE 2021

Ponga de su parte. #BeCyberSmart.

MENSAJES CLAVES DE 2021

Para ayudar a plantear temas de conversación, diseñar recursos e impulsar eventos con partes interesadas internas y externas, desglosamos el tema abarcador en cuatro mensajes semanales. Los mensajes claves a continuación se presentarán durante todo el mes para ayudar a impulsar los eventos, los recursos y las actividades que CISA y NCSA ejecutan, y hemos incluido posibles temas para ayudar a arrancar sus propios esfuerzos del Mes de Concienciación sobre Seguridad Cibernética.

- **Semana 1: Sea cibernéticamente inteligente**
Tome medidas sencillas para mantener seguras nuestras vidas digitales.
- **Semana 2: ¡Luche contra el phishing!**
Aprenda a reconocer y denunciar intentos de phishing para evitar ataques de ransomware y otros programas maliciosos.
- **Semana 3: Explore. Experimente. Comparta.**
Conmemore la [Cybersecurity Career Awareness Week](#) de la Iniciativa Nacional para Educación sobre Seguridad Cibernética (NICE, por sus siglas en inglés) y la fuerza laboral global de seguridad cibernética.
- **Semana 4: La seguridad cibernética primero**
Explore cómo la importancia de la seguridad cibernética y de mantenerse seguro en Internet sigue creciendo mientras nosotros continuamos a operar virtualmente en nuestro trabajo y en nuestras vidas personales.

CÓMO INVOLUCRAR A OTROS

Esta sección provee consejos para difundir los mensajes de concientización sobre seguridad cibernética para asegurar que su campaña para el Mes de Concientización sobre Seguridad Cibernética llegue a sus públicos destinatarios. La meta de la campaña de 2021 es fomentar la responsabilidad personal y cambios positivos en el comportamiento en cuanto a la seguridad cibernética. Para garantizar el éxito este octubre, tenga en cuenta esta meta cuando está creando recursos, desarrollando actividades y planificando eventos.

IDEAS PARA INVOLUCRAR A OTROS

- Aporte su voz y sus recursos a las conversaciones en las redes sociales con las etiquetas #BeCyberSmart y #CybersecurityAwarenessMonth
- Incluya un mensaje sobre la importancia de la seguridad cibernética en sus boletines, correos y páginas web durante el mes de octubre
- Organice un evento o una reunión para examinar los asuntos locales y relevantes de seguridad cibernética
- Organice, proporcione o promocióne oportunidades de capacitaciones y ejercicios sobre seguridad cibernética para sus partes interesadas internas y externas
- Participe en capacitaciones o ejercicios locales o virtuales para mejorar la seguridad cibernética y la resistencia de su organización
- Use las hojas de consejos disponibles en cisa.gov/cybersecurity-awareness-month para leer sobre varios temas de seguridad cibernética
 - Ya sea que esté en el trabajo o en la casa, estas hojas de consejos ofrecen algo útil para todos
- Hágase amigo de la Campaña STOP. THINK. CONNECT.™ en cisa.gov/stopthinkconnect
- Los profesionales de seguridad cibernética pueden comprometerse a ayudar a las comunidades vulnerables #SecureTogether y ayudarles a mejorar su posición de seguridad cibernética mediante las acciones claves en www.cybercrimesupport.org

CONSEJOS PRINCIPALES PARA COMPARTIR DURANTE EL MES DE CONCIENTIZACIÓN SOBRE SEGURIDAD CIBERNÉTICA

- **Duplique su protección de sus credenciales.** Habilite la autenticación por múltiples factores (MFA, por sus siglas en inglés) para todas sus cuentas y dispositivos 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 [Multi-Factor Authentication \(MFA\) How-to-Guide](#).
- **Altere su protocolo para sus 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 [Creating a Password Tip Sheet](#).

- **Si se conecta, debe proteger.** Ya sea su computadora, teléfono inteligente, dispositivo de juegos u otros dispositivos de las redes, la mejora de defensa contra los virus y los programas maliciosos es la actualización a las últimas versiones de los programas de seguridad, los navegadores web y los sistemas operativos. Inscríbese para actualizaciones automáticas, si puede, y proteja sus dispositivos con software antivirus. Para más información, lea la [Phishing Tip Sheet](#).
- **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 sospechoso, no responda y no haga clic en los enlaces o los adjuntos en el correo electrónico. Cuando esté disponible, use la opción de "denunciar phishing" o "denunciar" para ayudar a su organización o su proveedor de correo electrónico a bloquear otros correos electrónicos sospechosos antes de que lleguen a su buzón de entrada.
- **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 [Social Media Cybersecurity Tip Sheet](#).
- **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 virtual 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.

RECURSOS DE SEGURIDAD CIBERNÉTICA

A continuación, se proveen recursos útiles para usar tanto durante octubre como durante el resto del año. Explore estos sitios para encontrar contenido para usar en blogs, artículos y mensajes dentro de sus organizaciones y con públicos externos.

- La Alianza Nacional de Seguridad Cibernética (NCSA, por sus siglas en inglés) desarrolla alianzas público-privadas fuertes para crear e implementar labores de educación y sensibilización amplias para capacitar a los usuarios en casa, el trabajo y las escuelas con la información que necesitan para mantenerse seguros a sí mismos y a sus organizaciones, sistemas e información confidencial en Internet y para promover una cultura de seguridad cibernética. Para eventos recomendados de NCSA, haga clic: <https://staysafeonline.org>
- Impulsada por el Departamento de Seguridad Nacional de los EE. UU., la ["Be Cyber Smart" campaign](#) se ha diseñado para inspirar a la generación de estadounidenses jóvenes a responsabilizarse de su propia seguridad cibernética. Aprenda sobre los fundamentos de la seguridad cibernética, las estafas más comunes y cómo denunciar incidentes de seguridad cibernética en la página web de la campaña.
- ¿Busca información sobre un puesto o curso específico de seguridad cibernética? [The National Initiative for Cybersecurity Careers and Studies](#) (NICCS, por sus siglas en inglés) es un recurso nacional para educación, capacitación y desarrollo de la fuerza laboral de seguridad cibernética. NICCS ofrece herramientas e información para profesionales actuales y futuros de seguridad cibernética, desde los alumnos de K-12 y sus docentes hasta los empleados Federales hasta los Veteranos y personas que cambian de carrera. Estas herramientas y recursos están disponibles para cualquier persona que busque más información sobre el campo de seguridad cibernética, cómo avanzar en una carrera de seguridad cibernética y más.

CANALES DE COMUNICACIONES

Las etiquetas oficiales del Mes de Concientización sobre Seguridad Cibernética de 2021 son #BeCyberSmart y #CybersecurityAwarenessMonth. Aportar mayor visibilidad a la participación de usted y de su organización al aprovechar de estas etiquetas antes y durante el mes de octubre para promocionar y participar en las actividades y eventos de la campaña.

EJEMPLO DE UN CALENDARIO DE COMUNICACIONES

Use el calendario de comunicaciones a continuación para ayudar a planificar sus esfuerzos de sensibilización y ejecución desde ahora hasta el fin del Mes de Concientización sobre Seguridad Cibernética. Está destinado para servir de guía solamente y no está destinado para restringir o limitar sus actividades.

AGOSTO

- Para empezar el Mes de Concientización sobre Seguridad Cibernética, planifique entre el departamento de mercadotecnia y la dirección las actividades y el involucramiento para el mes de octubre, incluyendo posibles comunicaciones de la compañía, noticias e investigaciones que se podrían publicar durante el mes.
- **19 de agosto:** [Pida materiales de sensibilización sobre seguridad cibernética al por mayor](#) del Comisión Federal de Comercio (FTC, por sus siglas en inglés) para distribución durante octubre
- **27 de agosto:** Esta fecha es el último día para invitar a un representante de CISA o agencias Federales locales para hablar con sus empleados sobre la seguridad en Internet. Solicite oradores de CISA en la sección de "Request a CISA Speaker" en <http://www.cisa.gov/contact-us>

SEPTIEMBRE

- **1 de septiembre:** Cree un cronograma de comunicaciones digitales para publicaciones en redes sociales, blogs y correos electrónicos de la compañía y sus ejecutivos además de otras promociones relacionadas con el Mes de Concientización sobre Seguridad Cibernética durante el mes
- **20 de septiembre:** Empiece a contar los días durante las últimas dos semanas antes del Mes de Concientización sobre Seguridad Cibernética en sus canales de redes sociales
- **21 de septiembre:** Envíe un correo electrónico a sus empleados para anunciar su involucramiento en la campaña e indicar cómo su compañía se involucrará ahora y durante el Mes de Concientización sobre Seguridad Cibernética
- **30 de septiembre:** Exhiba gráficos del Mes de Concientización sobre Seguridad Cibernética en su negocio en áreas concurridos o en la página web (o las páginas web) de su organización
- **30 de septiembre:** Organice un evento durante el almuerzo para que los empleados puedan hablar sobre las políticas de seguridad cibernética y uso aceptable de la compañía y compartir la presentación inicial del Mes de Concientización sobre Seguridad Cibernética con sus empleados

OCTUBRE

- **1 de octubre:** Trabaje con la dirección de su organización para emitir una proclamación oficial de la compañía en apoyo del #CyberMonth y su compromiso a Poner de su parte. #BeCyberSmart.
- **1 de octubre:** Envíe una carta para clientes en la que destaca la participación del negocio en el Mes de Concientización sobre Seguridad Cibernética y se proveen consejos útiles de seguridad cibernética para que los clientes puedan #BeCyberSmart.
- **1 de octubre:** Envíe/ programe la primera serie de consejos o diarios en redes sociales/para empleados sobre cómo mantenerse seguro en Internet
- **4 de octubre:** Emita un comunicado de prensa de la compañía sobre el mes (actualizaciones de productos u ofertas, logros de los clientes, etc.)
- **11 de octubre:** Envíe/ programe la segunda serie de consejos o diarios en redes sociales/para empleados sobre cómo mantenerse seguro en Internet
- **18 de octubre:** Envíe/ programe la tercera serie de consejos o diarios en redes sociales/para empleados sobre cómo mantenerse seguro en Internet y cómo unirse a la fuerza laboral cibernética
- **19 de octubre:** Realizar una simulación de phishing con los empleados con [CISA's Cyber Hygiene Services](#)
- **25 de octubre:** Envíe/ programe la cuarta serie de consejos o diarios en redes sociales/para empleados sobre cómo mantenerse seguro en Internet

- **26 de octubre:** Organice un evento para Colaboradores del Mes de Concientización sobre Seguridad Cibernética para sus empleados y/o su comunidad local
- **28 de octubre:** Envíe una última distribución de materiales sobre seguridad en Internet que destacan la importancia de ser cibernéticamente inteligente todo el año
- **29 de octubre:** Envíe a los empleados un correo electrónico que resume la información que han aprendido durante el mes - podría proveer premios pequeños a los que se desempeñaron bien durante las actividades o se involucraron activamente

COMUNICACIONES EN LAS REDES SOCIALES

A continuación, se proveen unos ejemplos de publicaciones para redes sociales para promocionar el Mes de Concientización sobre Seguridad Cibernética en su organización. CISA y NCSA le exhortan a publicarlas en sus canales de comunicaciones en Internet desde ahora hasta el fin de octubre.

TWITTER:

Semana de lanzamiento:

#CyberMonth ha vuelto este octubre para su 18º año para educar a la Nación sobre la seguridad cibernética y cómo todos los estadounidenses pueden ser más seguros en Internet. Aprenda cómo puede Poner de su parte #BeCyberSmart en cisa.gov/cybersecurity-awareness-month

Semana 1 – Sea cibernéticamente inteligente:

Ponga de su parte #BeCyberSmart! Durante la primera semana del Mes de Concientización sobre Seguridad Cibernética estaremos explorando los puntos básicos de la seguridad cibernética para enseñarles cómo pueden asegurar de mejor manera sus vidas digitales y mejorar la seguridad de sus dispositivos. #CyberMonth #cybersecurity #InformationSecurity

Semana 2 – ¡Luche contra el phishing!:

¡Luche contra el phishing! Esta semana, el Mes de Concientización sobre Seguridad Cibernética se enfocará en cómo los individuos pueden detectar intentos de phishing. El phishing muchas veces conlleva a vulnerabilidades que pueden resultar en el ransomware u otros tipos de programas maliciosos. #FightThePhish #Phishing #Ransomware #BeCyberSmart #CyberMonth

Semana 3 - Explore. Experimente. Comparta.:

Esta semana, celebre la Semana de Concientización sobre Carreras de Seguridad Cibernética con CISA y la Iniciativa Nacional para la Educación sobre Seguridad Cibernética (NICE, por sus siglas en inglés). Esta semana, presentaremos sus aportaciones e innovaciones. El desarrollo de una fuerza laboral de seguridad cibernética aumentará la seguridad. #CyberMonth #CyberCareer

Semana 4 – La seguridad cibernética primero:

Es la última semana del Mes de Concientización sobre Seguridad Cibernética, usted debe continuar a poner de su parte y #BeCyberSmart! Las acciones de hoy afectan nuestro futuro. La seguridad cibernética es una labor de todo el año que se ha vuelto una consideración más importante para la manera en que trabajamos, aprendemos y vivimos. #CyberMonth #CybersecurityFirst

FACEBOOK:

Semana de lanzamiento:

El Mes de Concientización sobre Seguridad Cibernética vuelve para su 18º año en octubre de 2021. Cybersecurity Awareness Month Página web (cisa.gov/cybersecurity-awareness-month) destaca la necesidad de educar a individuos y organizaciones sobre la importancia de la seguridad cibernética y así asegurar que todos los estadounidenses cuenten con los recursos necesarios para estar más seguros en Internet.

- **Semana 1: Sea cibernéticamente inteligente**
- **Semana 2: ¡Luche contra el phishing!**
- **Semana 3: Explore. Experimente. Compartir. – Semana de Concientización sobre Carreras de Seguridad Cibernética**
- **Semana 4: La seguridad cibernética primero**

#BeCyberSmart #CyberMonth #Cybersecurity #InfoSec #InformationSecurity #Cybersecurity #StopThinkConnect
#HomeSecurity #InfoSecurity #NetworkSecurity #NetSec

Semana 1 – Sea cibernéticamente inteligente:

Ponga de su parte #BeCyberSmart! El primer tema semanal del Mes de Concientización sobre Seguridad Cibernética explorará los fundamentos de la seguridad cibernética para educar a los Estados Unidos sobre cómo poner de su parte y #BeCyberSmart! Unas medidas sencillas pueden ayudar a asegurar sus vidas digitales y mejorar la seguridad de los dispositivos conectados a Internet.

Los eventos de esta semana incluirán ____, ____ y _____. Para más información, visite la página web del Cybersecurity Awareness Month: cisa.gov/cybersecurity-awareness-month.

#CyberMonth #Cybersecurity #InfoSec #InformationSecurity #Cybersecurity #StopThinkConnect #HomeSecurity
#InfoSecurity #NetworkSecurity #NetSec

Semana 2 – ¡Luche contra el phishing!:

¡Luche contra el phishing! Esta semana, el Mes de Concientización sobre Seguridad Cibernética se enfocará en cómo los individuos pueden detectar posibles intentos de phishing. El phishing muchas veces conlleva a vulnerabilidades que pueden resultar en el ransomware u otros tipos de programas maliciosos. Reduzca sus posibilidades de ser víctima de ataques de phishing.

Los eventos de esta semana incluirán ____, ____ y _____. Aprenda más sobre phishing en la página web del Cybersecurity Awareness Month: cisa.gov/cybersecurity-awareness-month.

#Phishing #Ransomware #Malware #respond #recover

Semana 3 - Explore. Experimente. Comparta.:

Esta semana, celebre la Semana de Concientización sobre Carreras de Seguridad Cibernética con CISA y la Iniciativa Nacional para la Educación sobre Seguridad Cibernética (NICE, por sus siglas en inglés). Los profesionales de seguridad cibernética juegan un papel importante en la sociedad y seguridad globales. Esta semana, presentaremos sus aportaciones e innovaciones. El desarrollo de una fuerza laboral global de seguridad cibernética aumenta la seguridad de cada nación, podemos explicar cómo.

#ExploreExperienceShare #CyberMonth #Cybersecurity #InfoSec #InformationSecurity #Cybersecurity #StopThinkConnect
#HomeSecurity #InfoSecurity #NetworkSecurity #NetSec

Semana 4 – La seguridad cibernética primero:

Esta es la última semana del Mes de Concientización sobre Seguridad Cibernética, pero usted siempre debe tratar de poner de su parte y #BeCyberSmart. Lo que hacemos hoy puede afectar el futuro de la seguridad cibernética personal, del consumidor y de los negocios. La seguridad cibernética se está volviendo una consideración más importante para la manera en que trabajamos, aprendemos y jugamos. La seguridad cibernética es una labor de todo el año y debe ser una de nuestras primeras consideraciones cuando creamos o compramos dispositivos nuevos o servicios conectados.

Use la etiqueta #BeCyberSmart para unirse a la conversación sobre el Mes de Concientización sobre Seguridad Cibernética.

#BeCyberSmart #CybersecurityFirst #CyberMonth #Cybersecurity #InfoSec #InformationSecurity #Cybersecurity #StopThinkConnect
#HomeSecurity #InfoSecurity #NetworkSecurity #NetSec

INSTAGRAM:

Semana de lanzamiento:

El Mes de Concientización sobre Seguridad Cibernética ha vuelto este octubre para su 18º año para ayudar a educar a la Nación sobre la seguridad cibernética y cómo todos los estadounidenses pueden ser más seguros en Internet. Aprenda cómo puede Poner de su parte #BeCyberSmart en cisa.gov/cybersecurity-awareness-month.

-
-
-

#CyberMonth #Cybersecurity #BeCyberSmart #InfoSec #InformationSecurity #Cybersecurity #StopThinkConnect
#HomeSecurity #InfoSecurity #NetworkSecurity #NetSec

Semana 1 – Sea cibernéticamente inteligente:

Ponga de su parte #BeCyberSmart! Durante la primera semana del Mes de Concientización sobre Seguridad Cibernética estaremos explorando los puntos básicos de la seguridad cibernética para enseñarles cómo pueden asegurar de mejor manera sus vidas digitales y mejorar la seguridad de sus dispositivos. #CyberMonth #cybersecurity #InformationSecurity

Únase a la conversación sobre el Mes de Concientización sobre Seguridad Cibernética. Puede contribuir a la conversación con la etiqueta #BeCyberSmart.

-
-
-

#CyberMonth #Cybersecurity #BeCyberSmart #InfoSec #InformationSecurity #Cybersecurity #StopThinkConnect
#HomeSecurity #InfoSecurity #NetworkSecurity #NetSec

Semana 2 – ¡Luche contra el phishing!:

¡Luche contra el phishing! Esta semana, el Mes de Concientización sobre Seguridad Cibernética se enfocará en cómo los individuos pueden detectar intentos de phishing. El phishing muchas veces conlleva a vulnerabilidades que pueden resultar en el ransomware u otros tipos de programas maliciosos.

Use la etiqueta #BeCyberSmart para unirse a la conversación sobre el Mes de Concientización sobre Seguridad Cibernética.

-
-
-

#FightThePhish #Phishing #Ransomware #CyberMonth #Cybersecurity #BeCyberSmart #InfoSec
#InformationSecurity #Cybersecurity #StopThinkConnect #HomeSecurity #InfoSecurity #NetworkSecurity #NetSec

Semana 3 - Explore. Experimente. Comparta.:

Esta semana, celebre la Semana de Concientización sobre Carreras de Seguridad Cibernética con CISA y la Iniciativa Nacional para la Educación sobre Seguridad Cibernética (NICE, por sus siglas en inglés). Esta semana, presentaremos sus aportaciones e innovaciones. El desarrollo de una fuerza laboral de seguridad cibernética aumentará la seguridad.

-
-
-

#CyberCareers #CyberMonth #Cybersecurity #BeCyberSmart #InfoSec #InformationSecurity #Cybersecurity #StopThinkConnect
#HomeSecurity #InfoSecurity #NetworkSecurity #NetSec

Semana 4 – La seguridad cibernética primero:

Es la última semana del Mes de Concientización sobre Seguridad Cibernética, usted debe continuar a poner de su parte y #BeCyberSmart! Las acciones de hoy afectan nuestro futuro. La seguridad cibernética es una labor de todo el año que se ha vuelto una consideración más importante para la manera en que trabajamos, aprendemos y vivimos.

-
-
-

#CyberMonth #Cybersecurity #BeCyberSmart #InfoSec #InformationSecurity #Cybersecurity #StopThinkConnect
#HomeSecurity #InfoSecurity #NetworkSecurity #NetSec

LINKEDIN:

Semana de lanzamiento:

Este octubre marca el 18º año del Mes de Concientización sobre Seguridad Cibernética. Cada año, la campaña trabaja para educar a la Nación sobre la importancia de la seguridad cibernética y así asegurar que todos los estadounidenses cuenten con los recursos necesarios para estar más seguros en Internet.

¡Los individuos y las compañías pueden involucrarse en el Mes de Concientización sobre Seguridad Cibernética al usar los recursos de CISA para crear sus propias campañas de sensibilización! Los colaboradores pueden usar los temas semanales de este año para crear sus propias campañas de sensibilización.

- **Semana 1: Sea cibernéticamente inteligente**
- **Semana 2: ¡Luche contra el phishing!**
- **Semana 3: Explore. Experimente. Compartir. – Semana de Concientización sobre Carreras de Seguridad Cibernética**
- **Semana 4: La seguridad cibernética primero**

¡Aprenda más sobre la campaña en cisa.gov/cybersecurity-awareness-month/!

Semana 1 – Sea cibernéticamente inteligente:

#BeCyberSmart es el primer tema semanal del Mes de Concientización sobre Seguridad Cibernética y explorará los fundamentos de la seguridad cibernética para educar a las organizaciones sobre cómo poner de su parte y #BeCyberSmart! Unas medidas sencillas pueden ayudar a asegurar sus vidas digitales y mejorar la seguridad de los dispositivos conectados a Internet.

Los eventos de esta semana incluirán ____, ____ y _____. Para más información, visite la página web del Cybersecurity Awareness Month: cisa.gov/cybersecurity-awareness-month/.

#CyberMonth #Cybersecurity #InfoSec #InformationSecurity #Cybersecurity #StopThinkConnect
#HomeSecurity #InfoSecurity #NetworkSecurity #NetSec

Semana 2 – ¡Luche contra el phishing!:

¡Luche contra el phishing! Esta semana, el Mes de Concientización sobre Seguridad Cibernética se enfocará en cómo los individuos pueden detectar posibles intentos de phishing. El phishing muchas veces conlleva a vulnerabilidades que pueden resultar en el ransomware u otros tipos de programas maliciosos. Reduzca las posibilidades de que su compañía u organización sea víctima de ataques de phishing.

Los eventos de esta semana incluirán ____, ____ y _____. Aprenda más sobre phishing en la página web del Cybersecurity Awareness Month: cisa.gov/cybersecurity-awareness-month/.

Semana 3 - Explore. Experimente. Comparta.:

Esta semana, celebre la Semana de Concientización sobre Carreras de Seguridad Cibernética con CISA y la Iniciativa Nacional para la Educación sobre Seguridad Cibernética (NICE, por sus siglas en inglés). Los profesionales de seguridad cibernética juegan un papel importante en la sociedad y seguridad globales. Esta semana, presentaremos sus aportaciones e innovaciones. Construir una fuerza laboral global de seguridad cibernética aumenta la seguridad de cada nación; únase a nosotros para aprender por qué.

Semana 4 – La seguridad cibernética primero:

Esta es la última semana del Mes de Concientización sobre Seguridad Cibernética, pero usted siempre debe tratar de poner de su parte y #BeCyberSmart. Lo que hacemos hoy puede afectar el futuro de la seguridad cibernética personal, del consumidor y de los negocios. La seguridad cibernética se está volviendo una consideración más importante para la manera en que trabajamos, aprendemos y jugamos. La seguridad cibernética es una labor de todo el año y debe ser una de las primeras consideraciones de las organizaciones cuando crean o compran dispositivos nuevos o servicios conectados.

Los eventos de esta semana incluirán ____, ____ y _____. Aprenda más sobre phishing en la página web del Cybersecurity Awareness Month: cisa.gov/cybersecurity-awareness-month/.

EJEMPLO DE UNA ENTRADA PARA SU BLOG



CAMPAÑA DEL MES DE CONCIENTIZACIÓN SOBRE SEGURIDAD CIBERNÉTICA DE 2021

Ahora en su 18º año, el Mes de Concientización sobre Seguridad Cibernética continúa a fomentar sensibilización sobre la importancia de la seguridad cibernética en nuestra Nación. El Mes de Concientización sobre Seguridad Cibernética, celebrado cada octubre, es un esfuerzo colaborativo entre el gobierno y la industria para asegurar que todas las personas de la Nación cuenten con los recursos necesarios para estar más seguras en Internet.

PONGA DE SU PARTE. #BECYBERSMART.

Cada año, la [Cybersecurity and Infrastructure Security Agency \(CISA\)](#) y la [National Cyber Security Alliance \(NCSA\)](#) presiden el Mes de Concientización sobre Seguridad Cibernética para comunicar un mensaje claro sobre la importancia de la alianza entre el gobierno y la industria, desde la Casa Blanca al individuo.

El tema perenne—**Ponga de su parte. #BeCyberSmart.**—exhorta a los individuos y a las organizaciones a responsabilizarse de sus funciones para proteger su parte del ciberespacio y enfatiza la responsabilidad personal y la importancia de tomar medidas proactivas para aumentar la seguridad cibernética.

MENSAJES SEMANALES

Para ayudar a ustedes y sus organizaciones a crear una campaña eficaz de sensibilización sobre seguridad cibernética, CISA y NCSA han creado cuatro temas semanales de enfoque para el Mes de Concientización sobre Seguridad Cibernética:

- **Semana 1: Sea cibernéticamente inteligente**
La primera semana explora los puntos básicos de la seguridad cibernética: cómo unas medidas sencillas pueden ayudar a asegurar sus vidas digitales, cómo mejorar la seguridad de dispositivos inteligentes y con conexión a Internet y cómo otros fundamentos pueden ayudar a reducir los riesgos cibernéticos.
- **Semana 2: ¡Luche contra el phishing!**
La segunda semana se enfocará en cómo los individuos pueden detectar posibles intentos de phishing—los cuales frecuentemente conllevan a vulnerabilidades que pueden resultar en el ransomware u otros tipos de programas maliciosos. Se ofrecerán consejos sobre cómo los individuos pueden reducir las posibilidades de ser víctima de ataques de phishing—al denunciar o eliminar actividades sospechosas—también cómo responder o recuperarse de éstos.
- **Semana 3: Explore. Experimente. Comparta.**
En colaboración con la Iniciativa Nacional para la Educación sobre Seguridad Cibernética (NICE, por sus siglas en inglés, la tercera semana celebra la Semana de Concientización sobre Carreras de Seguridad Cibernética. Esta semana ilustrará

cómo los profesionales de seguridad cibernética juegan un papel importante en la sociedad y seguridad globales y enfocará la atención en sus aportaciones e innovaciones. La semana también exhibe cómo construir una fuerza laboral global de seguridad cibernética aumenta la seguridad de cada nación y fomenta la prosperidad económica.

- **Semana 4: La seguridad cibernética primero**

La última semana enfatizará que la seguridad cibernética debe ser una prioridad y no una idea adicional, y examinará cómo lo que hacemos hoy puede afectar el futuro de la seguridad cibernética personal, del consumidor y de los negocios. Esta semana también destacará el hecho que la seguridad cibernética es una labor de todo el año y debe ser entre las primeras consideraciones de los individuos y las organizaciones cuando crean o compran dispositivos nuevos y servicios conectados.

Este mes en especial, le pedimos que no trate la seguridad cibernética como un tema tabú; hable con otros sobre cómo "Ser cibernéticamente inteligente" y asegúrese de compartir los recursos del Mes de Concientización sobre Seguridad Cibernética con toda su comunidad—con sus amigos, su familia y sus compañeros. Al hacer esto, todos podemos avanzar enormemente la protección de nuestros dispositivos.

Use la etiqueta **#BeCyberSmart** del Mes de Concientización sobre Seguridad Cibernética para ayudar a promocionar la sensibilización sobre la seguridad cibernética. Además, asegúrese de seguir visitando la [página web](#) para aprender más sobre los próximos esfuerzos del Mes de Concientización sobre Seguridad Cibernética en octubre.

EJEMPLO DE UN CORREO ELECTRÓNICO A CLIENTES Y AL PERSONAL

A continuación, se provee un ejemplo de un correo electrónico que usted y su organización pueden usar para anunciar y promocionar el Mes de Concientización sobre Seguridad Cibernética con sus clientes y dentro de su propia organización.

CISA y NCSA le exhortan a comunicar los mensajes a sus partes interesadas y su organización desde ahora hasta el fin del mes de octubre.

Ejemplo de un correo electrónico a los clientes:

Estimado(s)/a(s) <clientes o grupo de partes interesadas>,

[INTRODUCIR NOMBRE DE LA ORGANIZACIÓN] se une a la Campaña del Mes de Concientización sobre Seguridad Cibernética.

Cada octubre, el [Cybersecurity Awareness Month](#) continúa a fomentar la sensibilización sobre la importancia de la seguridad cibernética en toda nuestra Nación. Liderado por la [Cybersecurity and Infrastructure Security Agency \(CISA\)](#) y la [National Cybersecurity Alliance \(NCSA\)](#), el Mes de Concientización sobre Seguridad Cibernética comparte mensajes y temas semanales sobre la importancia de mantenerse seguro en Internet. El tema perenne – **Ponga de su parte. #BeCyberSmart** – exhorta a los individuos y a las organizaciones a responsabilizarse de sus funciones para proteger su parte del ciberespacio y enfatiza la responsabilidad personal y la importancia de tomar medidas proactivas para aumentar la seguridad cibernética.

Durante el último año y medio, nuestro mundo ya virtual dependió aún más del Internet. Organizaciones como **[INTRODUCIR NOMBRE DE LA ORGANIZACIÓN]** e individuos como usted han usado el Internet más que nunca - para socializar, para hacer negocios y para divertirse.

Aunque una presencia aumentada en Internet puede ser positiva, el Mes de Concientización sobre Seguridad Cibernética exhorta a todos a responsabilizarse más de su actividad aumentada en Internet y de las prácticas de seguridad importantes correspondientes. La seguridad virtual de nuestra comunidad y, finalmente, de nuestra nación, depende de nuestras prácticas personales de seguridad en Internet.

La seguridad cibernética es importante para **[INTRODUCIR NOMBRE DE LA ORGANIZACIÓN]** y nos hemos comprometido a ayudar a nuestro clientes a ser más resistentes. Durante octubre, aprenderá a hacer lo siguiente:

- **Ser cibernéticamente inteligente**

Tomar medidas sencillas para mantener seguras nuestras vidas digitales.

- **¡Luchar contra el phishing!**

Destacar los peligros de los intentos de phishing—que pueden conllevar a ataques de ransomware u otros programas maliciosos—y cómo denunciar correos electrónicos sospechosos.

- **Explorar. Experimentar. Compartir.**

Celebrar la Cybersecurity Career Awareness Week de la Iniciativa Nacional de Educación sobre Seguridad Cibernética (NICE, por sus siglas en inglés) y la fuerza laboral global de seguridad cibernética y destacar cómo los individuos pueden convertirse en profesionales de seguridad cibernética

- **Piense en la seguridad cibernética primero**

Explore cómo la importancia de la seguridad cibernética y de mantenerse seguro en Internet sigue creciendo mientras nuestro mundo continúa a operar virtualmente tanto, en el trabajo y en la diversión.

Todos debemos abordar la seguridad cibernética con cuidado al responsabilizarnos, asegurar y proteger todas nuestras cuentas e información en Internet. [INTRODUCIR NOMBRE DE LA ORGANIZACIÓN] ofrece estos recursos gratuitos que usted puede utilizar para mantenerse seguro en Internet:

- La página web del Mes de Concientización sobre Seguridad Cibernética de CISA: cisa.gov/cybersecurity-awareness-month
- Fundamentos cibernéticos de CISA – buenas prácticas cibernéticas básicas para líderes empresariales: cisa.gov/cyber-essentials
- Aprenda más sobre las carreras en el campo cibernético con la Iniciativa Nacional para Carreras y Estudios Cibernéticos: niccs.cisa.gov

Si tiene preguntas sobre cómo [INTRODUCIR NOMBRE DE LA ORGANIZACIÓN] se involucra en la Campaña del Mes de Concientización sobre Seguridad Cibernética este año, escriba por correo electrónico a [INTRODUCIR CORREO ELECTRÓNICO DE LA PERSONA DE CONTACTO DE LA ORGANIZACIÓN PARA LA CAMPAÑA DEL MES DE CONCIENTIZACIÓN SOBRE SEGURIDAD CIBERNÉTICA]

<Firma>

Ejemplo de un correo electrónico al personal:

Estimado/a <nombre de la organización>,

¡[Cybersecurity Awareness Month](#) se celebrará en octubre de 2021! [INTRODUCIR NOMBRE DE LA ORGANIZACIÓN] se ha unido a la campaña anual organizada por la Agencia de Seguridad Cibernética y Seguridad de la Infraestructura (CISA, por sus siglas en inglés) y la Alianza Nacional de Seguridad Cibernética (NCSA, por sus siglas en inglés). La campaña enfatiza cómo los sectores público y privado pueden colaborar para poner de nuestra parte individual para construir un mundo seguro en Internet. Este año, continuamos con el tema abarcador de “**Ponga de su parte, #BeCyberSmart.**”

Muchos profesionales cibernéticos conocen los riesgos y asuntos de nuestro mundo siempre más virtual. En [INTRODUCIR NOMBRE DE LA ORGANIZACIÓN] queremos su ayuda para mejorar la posición cibernética y que use los conocimientos que obtiene en su trabajo para ayudar a otros a abordar la seguridad cibernética de manera segura y consciente.

Durante octubre, aprenderá sobre los cuatro mensajes semanales:

- **Semana 1: Sea cibernéticamente inteligente**
Cómo se puede tomar medidas sencillas para mantener seguras nuestras vidas digitales.
- **Semana 2: ¡Luche contra el phishing!**
Destacaremos los peligros de los intentos de phishing—que pueden conllevar a ataques de ransomware u otros programas maliciosos—y cómo denunciar correos electrónicos sospechosos.

- **Semana 3: Explore. Experimente. Comparta.**

Juntos celebraremos la Cybersecurity Career Awareness Week de la Iniciativa Nacional para la Educación sobre Seguridad Cibernética y la fuerza laboral global de seguridad cibernética, presentaremos nuestra propia feria de trabajos de seguridad cibernética y destacaremos las varias herramientas educativas de CICA.

- **Semana 4: La seguridad cibernética primero**

Explore cómo la importancia de la seguridad cibernética y de mantenerse seguro en Internet sigue creciendo mientras nuestro mundo continúa a operar virtualmente tanto, en el trabajo y en la diversión.

Cada uno de nosotros puede involucrarse este octubre para ayudar a los demás a estar más seguros en Internet. Ponga de su parte. #BeCyberSmart al utilizar los siguientes recursos:

La página web del Mes de Concientización sobre Seguridad Cibernética de CISA: cisa.gov/cybersecurity-awareness-month

Fundamentos cibernéticos de CISA – buenas prácticas cibernéticas básicas para líderes empresariales: cisa.gov/cyber-essentials

Aprenda más sobre las carreras en el campo cibernético con la Iniciativa Nacional para Carreras y Estudios Cibernéticos: niccs.cisa.gov

Si tiene preguntas sobre cómo [INTRODUCIR NOMBRE DE LA ORGANIZACIÓN] se involucra en la Campaña del Mes de Concientización sobre Seguridad Cibernética este año, escriba por correo electrónico a [INTRODUCIR CORREO ELECTRÓNICO DE LA PERSONA DE CONTACTO DE LA ORGANIZACIÓN PARA LA CAMPAÑA DEL MES DE CONCIENTIZACIÓN SOBRE SEGURIDAD CIBERNÉTICA] o si desea denunciar actividades sospechosas al departamento informático, escriba a [INTRODUCIR CORREO ELECTRÓNICO DEL DEPARTAMENTO INFORMÁTICO U OTRO CORREO ELECTRÓNICO RELEVANTE].

<Firma>