SECURE OUR WORLD

MES DE LA CONCIENTIZACIÓN SOBRE LA CIBERSEGURIDAD

Kit de herramientas para socios 2023

#CybersecurityAwarenessMonth
#SecureOurWorld

Presentado por

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY CISA

NATIONAL CYBERSECURITY ALLIANCE

ÍNDICE

¡BIENVENIDO AL VIGÉSIMO MES DE LA CONCIENTIZACIÓN SOBRE LA CIBERSEGURIDAD!

El Mes de la Concientización sobre la Ciberseguridad, que se celebra cada octubre, es una colaboración entre el gobierno y la industria privada para capacitar a todas las personas con el fin de proteger sus datos personales de las formas de delincuencia digital. Este kit de herramientas está destinado a crear recursos y comunicaciones para que las organizaciones hablen con sus empleados y clientes sobre cómo mantenerse seguros en línea.

La Agencia de Seguridad de Infraestructura y Ciberseguridad (Cybersecurity and Infrastructure Security Agency, CISA) y la Alianza Nacional de Ciberseguridad (National Cybersecurity Alliance, NCA) trabajan en colaboración durante todo el año en apoyo del Mes de la Concientización sobre la Ciberseguridad y crearon este kit de herramientas con una gran cantidad de recursos para ayudarlo a crear su propia campaña del Mes de la Concientización sobre la Ciberseguridad.

Este año es el vigésimo Mes de la Concientización sobre la Ciberseguridad. Al igual que la tecnología, el Mes de la Concientización sobre la Ciberseguridad ha crecido con rapidez. ¡Ahora las personas celebran el Mes de la Concientización sobre la Ciberseguridad en todo el mundo! A medida que nos volvemos más dependientes de la tecnología, cada vez es más importante fortalecer y adaptar nuestros hábitos de ciberseguridad. Este kit de herramientas proporciona varios recursos para mantenerlo a usted y a su comunidad seguros.

¡NUEVO LEMA PERMANENTE!

Nos complace anunciar el lanzamiento de un lema nuevo y perdurable que se utilizará durante todo el año y en los próximos eventos del Mes de la Concientización sobre la Ciberseguridad. Secure Our World (Proteger Nuestro Mundo) es una campaña nueva de concientización de CISA que tiene como objetivo promover ampliamente consejos y mejores prácticas de ciberseguridad para todas las personas durante todo el año. Los socios pueden comenzar a incorporar este lema en las próximas campañas y en las iniciativas durante todo el año, desde 2023 en adelante.

MENSAJES CLAVE

CISA y NCA promoverán estos cuatro comportamientos clave sobre ciberseguridad durante octubre. Estos comportamientos son simples y prácticos, tanto para individuos como para empresas, y proporcionan la base de los recursos, eventos y presentaciones del Mes de la Concientización sobre la Ciberseguridad:

CREE CONTRASEÑAS SEGURAS Y USE UN ADMINISTRADOR DE CONTRASEÑAS

ACTIVE LA AUTENTICACIÓN MULTIFACTOR

RECONOZCA Y DENUNCIE LA SUPLANTACIÓN DE IDENTIDAD

ACTUALICE SU SOFTWARE

TONO

En la narrativa del Mes de la Concientización sobre la Ciberseguridad se explica que la ciberseguridad no tiene por qué ser aterradora. Puede ser fácil adoptar hábitos seguros e incluso puede brindarle la tranquilidad de saber que su vida en línea es segura. Esto lo hacemos a través del siguiente tono de voz:

- **Positividad** - Las tácticas de intimidación no funcionan. En lugar de utilizar imágenes aterradoras de “piratas informáticos con sudaderas con capucha”, hable sobre los beneficios de reducir los riesgos cibernéticos y cómo fortalecer la ciberseguridad puede proteger lo que más importa en nuestras vidas.
- **Accesibilidad** - La ciberseguridad parece un tema complejo para muchos, pero en realidad solo consiste en personas. Logre que puedan identificar la ciberseguridad y comparta cómo cualquier persona puede aplicar una buena higiene cibernética.
- **Simplicidad** - evite la jerga y asegúrese de definir siglas
- **Vuelva a lo básico** - incluso practicar solo los conceptos básicos de higiene cibernética proporciona una base sólida de seguridad.

MATERIALES

Cada octubre, los promotores reciben un kit de herramientas con mensajes y contenido que le permiten contar con los recursos que necesita para crear su propia campaña de educación sobre ciberseguridad, ya sea en el trabajo, en casa o en su comunidad. Gracias al apoyo de nuestros socios, la campaña continúa creciendo año tras año, llegando a personas, familias, pequeñas y medianas empresas, corporaciones y a muchos otros lugares en todo el mundo.

Su kit de herramientas incluye lo siguiente:

- Esta guía en PDF del Mes de la Concientización sobre la Ciberseguridad, que incluye lo siguiente:
  - Detalles sobre los mensajes y las actividades de 2023
  - Formas en las que puede participar en el Mes de la Concientización sobre la Ciberseguridad
  - Cómo organizar sus propios eventos del Mes de la Concientización sobre la Ciberseguridad
- Plantilla de correo electrónico para promover el Mes de la Concientización sobre la Ciberseguridad entre sus empleados
- Plantilla de nota de prensa para anunciar su participación de manera pública
- Gráficos para las redes sociales
- Ejemplos de publicaciones para las redes sociales
- Fondo de videoconferencia de la marca
- Gráfico de firma de correo electrónico de la marca
- Infografía
- ¡Y próximamente!
  - Asesores de seguridad preventiva (Protective Security Advisor, PSA) y videos
  - Recursos traducidos
  - Hojas de consejos sobre cada uno de los cuatro mensajes clave

¡Continúe leyendo para obtener ideas sobre cómo utilizar estos materiales y desarrollar sus propias actividades!

UTILICE CONTRASEÑAS SEGURAS Y UN ADMINISTRADOR DE CONTRASEÑAS

A medida que nuestra vida en línea se expande, el usuario promedio pasó de tener solo unas pocas contraseñas a administrar más de 100. Son 100 contraseñas únicas que debe recordar, si aplica hábitos de contraseña seguros. Los administradores de contraseñas pueden evitarles a los usuarios la molestia de tener que recordar varias contraseñas y hacer que las cuentas sean más seguras recomendando contraseñas seguras y únicas, y almacenándolas todas en un solo lugar.

NUESTROS CONSEJOS Y RECOMENDACIONES

Usar una contraseña fácil de adivinar es como cerrar la puerta, pero dejar la llave en la cerradura. Los piratas informáticos pueden descifrar con rapidez las contraseñas débiles. La buena noticia es que las contraseñas seguras son una de las formas más fáciles de proteger sus cuentas contra la vulneración y reducir el riesgo de que alguien robe información confidencial, datos, dinero o incluso su identidad.

FORTALEZCA LAS CONTRASEÑAS CON ESTOS CONSEJOS

1. Cuanto más largas, más seguras: las contraseñas con al menos 16 caracteres son las más difíciles de descifrar.

2. Debe ser difícil de adivinar: Utilice una cadena aleatoria de letras, números y símbolos en mayúsculas y minúsculas. Si necesita memorizar una contraseña, cree una frase que pueda recordar y que tenga de 5 a 7 palabras no relacionadas. Sea creativo con la ortografía y agregue números o símbolos

3. Único en su tipo: utilice una contraseña única para cada cuenta.

Es imposible recordar contraseñas largas y únicas para cada una de nuestras cuentas. En lugar de escribirlas o reutilizar contraseñas débiles, **use un administrador de contraseñas.**

Los administradores de contraseñas generan contraseñas complejas y únicas por usted, las almacenan en un solo lugar y le avisan cuando tiene contraseñas débiles, repetidas o comprometidas. También pueden completar de manera automática las credenciales en sitios y aplicaciones mediante un complemento seguro en el navegador. Solo necesita recordar una contraseña maestra: la que le permite acceder al administrador de contraseñas. (Consejo: cree una “frase de contraseña” larga y que pueda recordar como se describió anteriormente y NUNCA escriba su contraseña maestra).

DATOS Y CIFRAS ADICIONALES

- Solo el 33 % de las personas crean contraseñas únicas para todas sus cuentas (NCA)
- Solo el 18 % de las personas ha descargado un administrador de contraseñas (NCA)

ACTIVE LA AUTENTICACIÓN MULTIFACTOR

En una encuesta reciente de la Alianza Nacional de Ciberseguridad, el 57 % de los encuestados dijeron que habían oído hablar de la autenticación multifactor (multifactor authentication, MFA), pero muchas personas no se dan cuenta de que la autenticación multifactor es una capa de protección muy importante para mantener las cuentas seguras. Este mes, le demostraremos a otras personas lo fácil que es activar la MFA, siempre que sea posible.

NUESTROS CONSEJOS Y RECOMENDACIONES

La MFA brinda seguridad adicional al proporcionar un método secundario que confirma su identidad cuando inicia sesión en cuentas. Por lo general, la MFA requiere que ingrese el código que se le envía a su teléfono o correo electrónico, o uno generado por una aplicación de autenticación. Las notificaciones automáticas también son métodos comunes de MFA. Este paso adicional evita que los usuarios no autorizados obtengan acceso a sus cuentas, incluso si su contraseña ha sido comprometida.

SIGA ESTOS PASOS PARA ACTIVAR LA MFA

- **Abra la configuración de su aplicación o cuenta**
  - Puede llamarse Configuración de cuenta, Configuración y privacidad o algo similar.
- **Active la autenticación multifactor**
  - También puede llamarse autenticación de dos factores, autenticación de dos pasos o algo similar.
- **Confírmelo**
  - Seleccione el método de MFA que desea usar entre las opciones proporcionadas. Algunos ejemplos son los siguientes:
    - Recibir un código por mensaje de texto o correo electrónico
    - Usar una aplicación de autenticación: estas aplicaciones telefónicas generan un nuevo código cada 30 segundos aproximadamente.
    - Usar datos biométricos: utiliza el reconocimiento facial o las huellas dactilares para confirmar su identidad.

DATOS Y CIFRAS ADICIONALES

- De las personas que ya conocen la MFA, el 79 % la había aplicado a sus cuentas en línea (NCA)
- De ese número, el 94 % dijo que todavía usa la MFA, lo que demuestra que una vez que la MFA está habilitada, los usuarios seguirán usándola (NCA)

RECONOZCA Y DENUNCIE LA SUPLANTACIÓN DE IDENTIDAD

Los ataques de suplantación de identidad se convirtieron en un problema cada vez más común para las organizaciones de todos los tamaños y pueden ser muy difíciles de detectar. Es importante que cada individuo se detenga y piense antes de hacer clic en un enlace o abrir un archivo adjunto y que sepa cómo detectar las señales de alerta. La guía del Mes de la Concientización sobre la Ciberseguridad 2023 proporciona las herramientas necesarias para reconocer e informar sobre la suplantación de identidad a su organización o proveedor de correo electrónico.

NUESTROS CONSEJOS Y RECOMENDACIONES

La suplantación de identidad ocurre cuando los delincuentes intentan que usted abra enlaces o archivos adjuntos dañinos que podrían robarle información personal o infectar dispositivos. Los mensajes de la suplantación de identidad o "señuelo" suelen llegar como un correo electrónico, mensaje de texto, mensaje directo en las redes sociales o una llamada telefónica. Estos mensajes a menudo están diseñados para que usted crea que provienen de una persona u organización de confianza y lo responda. ¡La buena noticia es que puede evitar la suplantación de identidad y mantener sus cuentas seguras!

SIGA ESTOS CONSEJOS PRINCIPALES:

1. Reconocer. Busque estos signos comunes:

- Lenguaje urgente o alarmante
- Solicitudes de envío de datos personales o financieros
- Mala redacción, errores ortográficos o lenguaje inusual
- Direcciones de correo electrónico, nombres de dominio o enlaces incorrectos (por ejemplo, amazan.com)

2. Informar. Si tiene sospechas de una suplantación de identidad, infórmelo para protegerse a usted mismo y a los demás.

- Conozca las pautas de la organización para denunciar la suplantación de identidad. Si su organización lo ofrece, puede encontrar opciones para presentar los informes mediante el botón "Informar spam" en la barra de herramientas o en la configuración de su correo electrónico.
- Para cuentas de correo electrónico personales, es posible que pueda denunciar el spam o la suplantación de identidad a su proveedor de correo electrónico haciendo clic derecho en el mensaje.

3. Eliminar. Elimine el mensaje. No responda ni haga clic en ningún archivo adjunto o enlace, tampoco en ningún enlace para "cancelar la suscripción". Solo bórrelo.

DATOS Y CIFRAS ADICIONALES

- El 72 % de los encuestados informó que verificaba si los mensajes eran legítimos (es decir, si no eran una estafa o suplantación de identidad), en comparación con el 15 % que informó que no lo había hecho (NCA)
- El 47 % de los participantes comentó que utilizaba la función para denunciar en una plataforma (por ejemplo, Gmail, Outlook) "muy a menudo" o "siempre" (NCA)

ACTUALICE SU SOFTWARE

Aproximadamente 2 de cada 5 encuestados dicen que “a veces”, “rara vez” o “nunca” instalan las actualizaciones de software (NCA). Una de las formas más sencillas de proteger las cuentas y la información es mantener el software y las aplicaciones actualizados. Cada cierto tiempo, se publican actualizaciones con el fin de solucionar los problemas de software y proporcionar parches de seguridad para vulnerabilidades conocidas. Este Mes de la Concientización sobre la Ciberseguridad, no presione el botón “Recordármelo más tarde”. Tome medidas para estar un paso adelante de los ciberdelincuentes.

NUESTROS CONSEJOS Y RECOMENDACIONES

Mantener el software actualizado es una manera sencilla de mejorar la seguridad digital. Para mayor comodidad, active las actualizaciones automáticas en la configuración de seguridad de su dispositivo o aplicación. Configúrelo y olvídelo!

MANTENGA EL SOFTWARE ACTUALIZADO CON ESTOS PASOS:

1. Esté atento a las notificaciones

Por lo general, los dispositivos y las aplicaciones le notificarán cuando estén disponibles las últimas actualizaciones de software, pero también es importante verificarlas con frecuencia. Las actualizaciones de software incluyen los sistemas operativos, los programas y las aplicaciones de los dispositivos. Es importante instalar TODAS las actualizaciones, en especial, para los navegadores web y software antivirus o que contengan información personal o financiera.

2. Instale las actualizaciones lo antes posible

Cuando se le notifique sobre actualizaciones de software, en especial las actualizaciones críticas, instálelas lo antes posible. ¡Los atacantes no esperarán, y usted tampoco debería hacerlo!

3. Active las actualizaciones automáticas

Con las actualizaciones automáticas, los dispositivos instalarán las actualizaciones tan pronto como estén disponibles. ¡Así de fácil! Para activar la función de las actualizaciones automáticas, busque en la configuración del dispositivo, que suele encontrarse en Software o Seguridad.

DATOS Y CIFRAS ADICIONALES

- El 36 % de los participantes de la encuesta informaron que instalaron las últimas actualizaciones y el software tan pronto como estuvieron disponibles (NCA).
- Entre los que informaron haber instalado las últimas actualizaciones en sus dispositivos, el 62 % había activado las actualizaciones automáticas (NCA).

DESARROLLO DE SU CAMPAÑA

En esta sección se proporcionan consejos acerca de cómo participar en el Mes de la Concientización sobre la Ciberseguridad y desarrollar su propia campaña. El objetivo del Mes de la Concientización sobre la Ciberseguridad es promover cambios de comportamiento positivos a través de mensajes simples y que brinden capacitación. Para garantizar el éxito este octubre, tenga en cuenta este objetivo al crear recursos y planificar actividades.

EN LA ORGANIZACIÓN

- **Correos electrónicos**: Envíe un correo electrónico a colegas, empleados, clientes o a su escuela con información sobre el mes. Describa cómo participará su organización. Destaque los comportamientos clave y los consejos que se proporcionan en este kit de herramientas. Para comenzar, consulte el “Ejemplo de correo electrónico de empleado” en este kit de herramientas.

- **Boletines**: Incorpore el Mes de la Concientización sobre la Ciberseguridad en un boletín. Utilice una copia del “Ejemplo de correo electrónico para los empleados”.

- **Concursos**: ¿trabaja con estudiantes? Organice un concurso de carteles o videos en el que los estudiantes puedan crear recursos informativos de seguridad en línea para su escuela y comunidad. ¡Exhiba las obras ganadoras y considere otorgar premios!

- **Puesto de información**: ¡Prepare una estación de información! Ya sea en el centro de estudiantes de la escuela o en la sala de descanso de una empresa, prepare un área para entregar hojas informativas y hablar con personas dentro de la organización o escuela.

- **Promoción**: Trabaje con los líderes para emitir un comunicado de prensa oficial, una proclamación o un anuncio en video para demostrar el apoyo de la organización. Los anuncios deben destacar lo que hace la empresa para practicar la ciberseguridad. Consulte el “Ejemplo de comunicado de prensa” en el kit de herramientas.

- **Evento**: Organice un evento o capacitación local o virtual para la organización. Analice las prácticas de seguridad inteligentes y las cuestiones relevantes de ciberseguridad, y permita que los participantes hagan preguntas relacionadas con la ciberseguridad. Continúe leyendo para obtener más consejos sobre cómo organizar un evento o una sesión de capacitación.

- **Ludificación**: Organice un juego o una competencia relacionado con la suplantación de identidad. Envíe correos electrónicos de suplantación de identidad falsos a sus empleados y premie a quienes detecten y denuncien la mayor cantidad de intentos de suplantación de identidad.

DESARROLLO DE SU CAMPAÑA

EN LA ORGANIZACIÓN (continuación)

- **Marca**: publique el logotipo del Mes de la Concientización sobre la Ciberseguridad en el sitio web interno o externo de la empresa.

- **Incentivos**: Emita una promoción de la empresa relacionada con el mes, como un descuento en un producto, una competencia o sorteos para los clientes.

- **Capacitación**: Realice una simulación de suplantación de identidad con los empleados. Recuerde premiar el comportamiento positivo y no castigar los errores. Considere ofrecer pequeños premios a quienes tengan un buen desempeño y participen en las actividades.

- **Folletos**: distribuya materiales de seguridad y hojas de consejos en línea. Proporcionamos una gran cantidad de materiales de dominio público disponibles para descargar e imprimir desde staysafeonline.org.

- **Resumen**: Al final del mes, envíeles a los empleados un correo electrónico destacando sus actividades, resultados y éxitos. Recapitule las mejores prácticas aprendidas a lo largo del mes.

EN CASA

- Comparta las hojas de consejos e imprima recursos para exhibirlos en áreas donde los miembros de la familia pasen tiempo en línea.

- Organice una “charla tecnológica” con la familia y analice cómo cada miembro de la familia puede proteger sus dispositivos, cuentas e información personal.

- Envíele un correo electrónico a amigos y familiares informándoles que octubre es el Mes de la Concientización sobre la Ciberseguridad y comparta consejos y recursos útiles, en especial, con grupos vulnerables, como adultos mayores y adolescentes.

- Cree una cultura de seguridad en su familia. Deje en claro a todos los miembros de la familia que deben sentirse cómodos compartiendo si hicieron clic en un enlace malicioso, descargaron algo que no debían o si cayeron en una estafa, en especial, en el caso de niños y adultos mayores.

ORGANIZACIÓN DE UN EVENTO O CAPACITACIÓN

¡Organizar un evento o una sesión de capacitación es más fácil de lo que piensa! A continuación, se presentan algunas ideas que lo ayudarán a empezar.

HÁGALO DE MANERA ENTRETENIDA

La ciberseguridad es un problema grave, pero no es necesario que nuestras conversaciones generen miedo. Realice eventos con contenido que capaciten a su audiencia. Intente utilizar el humor o la narración para involucrar a los alumnos y llamar su atención.

DEMUESTRE EL COMPROMISO DEL PERSONAL DIRECTIVO

Involucre a la alta dirección de la organización (director ejecutivo, director de sistemas de información, director de seguridad de la información) para enfatizar la importancia de la ciberseguridad en la organización y demostrar que la ciberseguridad es parte de la cultura corporativa.

HAGA QUE LA EXPERIENCIA DE APRENDIZAJE SEA INTERACTIVA Y ACCESIBLE

Adapte el evento a lo que es más importante en su organización, pero no tema ser creativo con las siguientes sugerencias.

- Realice demostraciones en vivo, por ejemplo, cómo utilizar una red privada virtual (Virtual Private Network, VPN) proporcionada por la empresa o cómo instalar una aplicación de autenticación aprobada por la empresa.
- Cree un ejercicio práctico en el que los equipos interdisciplinarios puedan representar un escenario y practicar sus estrategias de respuesta. Consulte los paquetes de ejercicios prácticos de CISA.
- Ponga a prueba el conocimiento de la audiencia con un juego o una encuesta.
- Brinde un tiempo para que la audiencia haga preguntas.
- Logre que la educación en ciberseguridad sea más accesible para los empleados al relacionar el tema con el hogar o la vida familiar, o con las necesidades específicas de su departamento o rol en la organización.

RECONOZCA Y RECOMPENSE EL COMPROMISO

Entregue premios a los participantes por su buen desempeño en los cuestionarios o por hacer preguntas. Al entregar regalos, dulces o tarjetas de regalo de la marca puede crear un evento divertido y atractivo.

- ¿Utiliza un proveedor de seguridad? ¡Consulte si tienen artículos gratis que puedan enviarle para que usted se los entregue a los empleados!

NO OLVIDE REALIZAR EL SEGUIMIENTO

Comuníquese con los participantes después del evento. Agradézcales por asistir e incluya los materiales y recursos en la presentación que utilizó durante el evento.

ADAPTE SU EVENTO

A continuación, se ofrecen consejos que le ayudarán a adaptar su evento con el Mes de la Concientización sobre la Ciberseguridad y solicitar oradores.

- Utilice el logotipo en los materiales promocionales, que incluyen los siguiente:
  - Invitaciones al evento
  - Carteles y telones de fondo
  - Materiales e impresiones del evento
- Utilice los recursos gratuitos de CISA, NCA y otras organizaciones, que se mencionan en la página “Recursos adicionales” de esta guía, como folletos o copias a petición para usar como contenido de la capacitación.
- Incluya el evento en el calendario comunitario de la NCA.
  - ¡Puede enviar cualquier evento público a nuestro sitio web! Envíe los siguientes detalles a info@staysafeonline.org:
    - Nombre del evento
    - Descripción
    - Fecha y hora
  - Ubicación
  - Sitio web y enlace de inscripción

SOLICITE UN ORADOR DE CISA

Para solicitar un orador de CISA, envíe el Formulario de solicitud de orador aquí. Las solicitudes de oradores se procesan de forma continua, y les recomendamos a los socios que soliciten oradores durante todo el año.

SOLICITE UNA PRESENTACIÓN DE LA ALIANZA NACIONAL DE CIBERSEGURIDAD

Este octubre, la Alianza Nacional de Ciberseguridad ofrece presentaciones divertidas e interactivas del Mes de la Concientización sobre la Ciberseguridad a organizaciones de todos los tamaños. Estas charlas informativas abordarán los “conceptos básicos cibernéticos” y mejorarán la capacitación interna y los eventos para empleados de su organización.

Al participar en estas charlas, los empleados obtendrán conocimientos valiosos para fortalecer las prácticas de ciberseguridad y contribuir a un entorno digital más seguro.

Para programar una charla, seleccione el horario deseado a través de nuestro formulario “Solicitar un orador”.

ENSÉÑELE A OTRAS PERSONAS CÓMO MANTENERSE SEGURAS EN LÍNEA

Incluso si no se considera un maestro, tiene algo que compartir con sus amigos, vecinos y otras personas de su comunidad. Considere ofrecerse como voluntario en un centro comunitario, un centro para adultos mayores, una escuela, una biblioteca o en un grupo de exploradores para enseñarles a otros los conceptos cibernéticos básicos. A continuación, se ofrecen algunos consejos que le ayudarán a preparar una charla sobre "Conceptos cibernéticos básicos"

- **Paciencia** - Comuníquese cuanto antes con los líderes de la comunidad para promover su presentación. Si desea dar una charla durante el Mes de la Concientización sobre la Ciberseguridad, considere comunicarse con seis meses de anticipación. ¿Le parece extraño? Muchos bibliotecarios, líderes de clubes y administradores escolares planifican eventos con mucha antelación, por lo que conviene tener en cuenta sus horarios y ser cortés en su planificación.

- **Enfoque en la audiencia** - ¡Comprenda el conocimiento tecnológico de su audiencia! Hable con el líder comunitario que programó su presentación para comprender cómo usan la tecnología dentro del club o de la organización y cómo podrían utilizarla en su vida cotidiana.

- **Materiales para llevar a casa** - cree una presentación de diapositivas o material complementario que las personas puedan llevarse a casa. Haga que su presentación también sirva como una guía de aprendizaje después de su partida. Bríndeles recursos a los que puedan acudir para obtener más ayuda, en especial, si tienen un incidente de ciberseguridad. Asegúrese de que sepan qué ayuda tienen disponible y con quién deben comunicarse: FBI, CISA, etc. Su trabajo es brindarles cierta educación y dejarles recursos, consejos y contactos para que los utilicen por su cuenta.

- **Capacitación y educación** - no utilice el miedo, la incertidumbre o la duda para expresar su punto de vista. Concéntrese en consejos y lenguaje sencillos, amigables y que capaciten. Evite la jerga y las siglas. Brinde información en su charla sin ser condescendiente. La personas quieren aprender. Proporcione explicaciones más detalladas según sea necesario.

- **Investigue** - hable con un líder de la comunidad sobre cuáles son sus mayores preocupaciones, temores o problemas. No continúe con una charla de 20 minutos sobre seguridad en la nube, si lo que realmente necesitan es entender cómo es un correo electrónico de suplantación de identidad. ¡Conozca a su audiencia!

Consulte el kit de herramientas para voluntarios y la serie de videos de NCA para obtener más consejos.

ÚNASE A LA CONVERSACIÓN EN LÍNEA

¡Una de las mejores maneras de participar es unirse a la conversación en línea! Le recomendamos que publique en los canales de las redes sociales antes y durante todo el mes de octubre.

- Publique consejos de seguridad en línea y contribuya con sus propios consejos y recursos en las redes sociales utilizando los hashtags:

#CybersecurityAwarenessMonth

#SecureOurWorld

- Utilice nuestras publicaciones y gráficos diseñados para las redes sociales antes y durante todo el mes. Puede personalizarlos con sus propios mensajes y logotipos.
- Reemplace o incorpore su imagen de perfil personal o de su empresa o la imagen de su anuncio en las plataformas de redes sociales con el logotipo del Mes de la Concientización sobre la Ciberseguridad durante todo el mes de octubre.
- Escriba publicaciones sobre ciberseguridad. Elija un tema que a usted y a su audiencia le resulte interesante o destaque uno de los comportamientos clave. Puede utilizar los artículos de ejemplo en el kit de herramientas.
- Siga a CISA y NCA en las redes sociales para recibir las últimas noticias acerca de seguridad en línea.

CISA	NCA
Twitter	Twitter
LinkedIn	LinkedIn
Facebook	Facebook
Instagram	Instagram
YouTube	YouTube

¡Recuerde que la educación en ciberseguridad no se limita a octubre! ¡Utilice estas ideas para capacitar a su organización y comunidad durante todo el año!

RECURSOS ADICIONALES

A continuación, se muestran recursos gratuitos que serán útiles durante octubre y durante todo el año. Explore estos sitios en busca de contenido para utilizar en blogs, artículos y boletines dentro de su organización y con audiencias externas.

Servicios de higiene cibernética de CISA - CISA ofrece varios servicios de escaneo y pruebas para ayudar a las organizaciones a reducir su exposición a las amenazas adoptando un enfoque proactivo para identificar y notificar a las organizaciones sobre amenazas existentes o emergentes.

Capacitación y ejercicios sobre ciberseguridad de CISA - la capacitación es esencial para mantener a los trabajadores informados sobre ciberseguridad. CISA se compromete a brindarle acceso a la nación a capacitación en ciberseguridad y materiales de desarrollo de la fuerza laboral para fomentar una nación cibernética más resiliente y capaz.

Cyber.org - Cyber.org permite que los educadores desde jardín de infantes hasta 12.° grado puedan enseñar información cibernética con confianza, lo que da como resultado estudiantes con las habilidades y la pasión necesarias para tener éxito en la fuerza laboral cibernética.

Campaña GetCyberSafe del Mes de la Concientización sobre la Ciberseguridad - cuando los ataques cibernéticos como la suplantación de identidad tienen éxito, pueden arruinarnos el día, por decirlo de alguna manera. Por este motivo, en este Mes de la Concientización sobre la Ciberseguridad, alentamos a los canadienses a arruinarle el día a un ciberdelincuente.

Mes Europeo de la Concientización sobre la Ciberseguridad en ENISA - el Mes Europeo de la Ciberseguridad (European Cybersecurity Month, ECSM) es la campaña anual de la Unión Europea dedicada a promover la ciberseguridad entre los ciudadanos y las organizaciones de la UE, y a proporcionar información actualizada sobre la seguridad en línea a través de la sensibilización y el intercambio de buenas prácticas.

Publicaciones gratuitas de la Comisión Federal de Comercio (Federal Trade Commission, FTC) - puede encontrar publicaciones gratuitas sobre estafas, privacidad, crédito y más en la FTC. Puede descargar e imprimir algunas copias o realizar pedidos más grandes.

Recursos y guías de la NCA - la Alianza Nacional de Ciberseguridad quiere que aprender más sobre ciberseguridad y seguridad en línea sea fácil para todos. Explore los artículos y otros recursos que necesita para crear conciencia en el hogar, el trabajo, la escuela o en toda su comunidad.

Semana de concientización sobre carreras en ciberseguridad de la Iniciativa Nacional para la Educación en Ciberseguridad (National Initiative for Cybersecurity Education, NICE) - únase a NICE para promover la concientización y la exploración de las carreras en ciberseguridad organizando un evento, participando en un evento cerca de usted o involucrando a los estudiantes con contenido de ciberseguridad.

PÓNGASE EN CONTACTO

AGENCIA DE CIBERSEGURIDAD Y SEGURIDAD DE LA INFRAESTRUCTURA

Como la Agencia de Defensa Cibernética de Estados Unidos y Coordinadora Nacional para la resiliencia y seguridad de la infraestructura crítica, CISA dirige el esfuerzo nacional para comprender, gestionar y reducir el riesgo de la infraestructura física y cibernética de la que dependen los estadounidenses, cada hora de cada día.

SITIO WEB

cisa.gov/cybersecurity-awareness-month

CONTACTO

AwarenessCampaigns@cisa.dhs.gov

COMUNÍQUESE CON SU OFICINA REGIONAL DE CISA VISITANDO
www.cisa.gov/about/regions

INFORMAR UN PROBLEMA CIBERNÉTICO
report@cisa.dhs.gov o (888) 282-0870.

ACERCA DE LA ALIANZA NACIONAL DE CIBERSEGURIDAD (NCA)

La Alianza Nacional de Ciberseguridad es una organización sin fines de lucro cuya misión es crear un mundo más seguro e interconectado. Apoyamos el uso seguro de toda la tecnología y educamos a todas las personas sobre la mejor manera de protegernos a nosotros mismos, a nuestras familias y a nuestras organizaciones contra el cibercrimen. Creamos asociaciones sólidas entre gobiernos y corporaciones para potenciar nuestro mensaje y fomentar un bien “digital” mayor.

SITIO WEB

staysafeonline.org

CONTACTO

info@staysafeonline.org