Formación y concienciación de los empleados

Ahora es el momento de recopilar los conocimientos que ha adquirido a lo largo del programa y compartirlos con sus compañeros. Como líder en ciberseguridad de su organización, conseguirá realizar cambios duraderos en su organización y en la cadena de valor global en general.

En esta sección, hemos incluido recursos clave para ayudarlo a comunicar las prácticas recomendadas de preparación cibernética en su organización para impulsar un cambio significativo. Encontrará plantillas de correo electrónico que puede copiar y personalizar, listas de verificación que puede compartir para que todos los miembros de su organización rindan cuentas y enlaces a recursos adicionales, tanto de CRI como de toda la comunidad de ciberseguridad, que pueden ofrecer orientación adicional a su equipo.

La implementación es el paso más importante del Programa de preparación cibernética porque es el momento en que el conocimiento se convierte en acción. Para ayudarle en este proceso, le hemos proporcionado los siguientes recursos que puede usar:

1. Plantillas de correo electrónico: utilice estas plantillas para presentar a sus empleados las cuatro políticas básicas y otros conceptos clave.

2. Módulos de formación de las cuatro políticas básicas: vídeos cortos de formación de las cuatro políticas básicas que se pueden distribuir fácilmente a los empleados

3. Presentaciones en PowerPoint de formación: presentaciones en PowerPoint para sesiones de formación de empleados

4. Materiales compartibles: carteles, campañas en redes sociales, guías, etc.

CRI ha descubierto que un enfoque sumamente personalizado es la mejor manera de lograr los máximos resultados de la formación. Comunicar claramente a los empleados no solo el valor para la empresa, sino también para ellos mismos, que pueden aportar los cursos sobre ciberseguridad proporcionará los mejores resultados.

Cuando tenga que decidir cuál es el método de comunicación mejor, tenga en cuenta el tamaño de su empresa y la cantidad de empleados. Las conversaciones cara a cara, las comunicaciones por correo electrónico o incluso los seminarios web programados para realizar un seguimiento y ayudar a los empleados durante el proceso de formación garantizarán un alto porcentaje de finalización.

Documento de certificación de formación

El Cyber Readiness Institute exige que todos los empleados y personal subcontratado reciban formación para obtener la certificación de preparación cibernética.

Al firmar y devolver este formulario de certificación, usted confirma que todos los empleados y personal subcontratado han recibido formación sobre las cuatro políticas principales de CRI y su papel en el plan de continuidad del negocio.

_____	_____
CEO	Líder en ciberseguridad
_____	_____
Fecha de la firma	Fecha de la firma

Recursos de formación

Plantillas de correo electrónico: Las siguientes plantillas de correo electrónico se pueden modificar y distribuir a todos los empleados para notificarles su nombramiento para el puesto de líder en ciberseguridad, las nuevas políticas de ciberseguridad de la organización y los próximos requisitos de formación. Es importante que el CEO envíe el primer correo electrónico para que los empleados entiendan la importancia de esta iniciativa.

1

Asunto: Mensaje de la dirección a los empleados sobre la preparación cibernética

Hola, equipo:

Los ciberataques son amenazas muy reales y presentes para [Nombre de la empresa] y las empresas a las que ofrecemos servicio. Es de vital importancia para el futuro de nuestro negocio que mejoremos nuestra preparación cibernética ahora. Es por eso que nos hemos asociado con Cyber Readiness Institute para proteger los datos de [Nombre de la empresa], los datos de nuestros clientes y vuestra información personal para que no se vean expuestos ni se utilicen con fines maliciosos.

He designado a [Nombre completo] como nuestros líderes en ciberseguridad. [Él/ella/ellos/ellas] guiarán a nuestro equipo a través del Programa de preparación cibernética, que adopta un enfoque práctico para aumentar la concienciación sobre la ciberseguridad centrándose en el comportamiento humano. A lo largo del programa, explicaremos las ciberamenazas comunes que puede sufrir nuestra empresa y desarrollaremos un manual de preparación cibernética para defendernos de ellas.

La realidad es que simplemente hacer clic en un enlace de correo electrónico sospechoso puede permitir que un agente malicioso acceda a nuestra red, accediendo así a los datos de nuestra empresa, los datos de nuestros clientes y vuestra información personal. Me comprometo a hacer que [Nombre de la empresa] sea más resiliente a la ciberseguridad previniendo los ataques y estando preparados cuando ocurra alguno. Gracias por acompañarme para apoyar a [Nombre completo] para garantizar que [Nombre de la empresa] esté preparada para la ciberseguridad.

Muchas gracias,

[Firma del CEO]

2

Asunto: Nuevas políticas de concienciación y formación sobre seguridad

¡Hola, equipo!

¡[NOMBRE DE LA ORGANIZACIÓN] se está preparando para la ciberseguridad. ¿Qué significa esto para nosotros?:

- Nuevas políticas para empleados: hemos añadido algunas políticas y protocolos nuevos a nuestro manual que ofrecen procedimientos y pautas para mejorar la seguridad aquí en [NOMBRE DE LA ORGANIZACIÓN]. Podéis consultar estas políticas aquí. [ENLACE]
- Líder en ciberseguridad designado: una persona responsable de liderar nuestro viaje de preparación cibernética.

Quizás os preguntéis qué significa estar preparado para la ciberseguridad. Estar preparado para la ciberseguridad significa ser inteligente con respecto a los hábitos tecnológicos y saber qué buscar para mantenerse seguro.

Los ciberdelincuentes saben cómo trabajamos la mayoría de nosotros y aprovechan estos hábitos comunes para burlar la sofisticada tecnología de ciberseguridad. De hecho, algunos comportamientos son el origen de la mayoría de las vulneraciones cibernéticas y de cómo los delincuentes logran abrirse paso. Afortunadamente, cuando sabemos qué hacer y qué no hacer en relación con estos cuatro problemas principales de ciberseguridad, la posibilidad de que estos métodos de ataque tengan éxito disminuye drásticamente.

- Contraseñas+
- Actualizaciones de software
- Phishing
- Almacenamiento e intercambio de datos

Bloquear estas cuatro áreas significa que los datos confidenciales relacionados con los clientes, proveedores y compañeros de trabajo de [NOMBRE DE LA ORGANIZACIÓN] están más seguros. Es por eso que enviaremos algunos correos electrónicos breves que ofrecerán información básica sobre los cuatro problemas de ciberseguridad y las cosas simples que todos podemos hacer para evitarlos y prevenirlos.

Tened en cuenta que el cumplimiento de la política y la formación de ciberseguridad son obligatorios. Estos correos electrónicos y solicitudes solo deberían tardar entre 10 y 15 minutos en completarse, y os pedimos que contactéis con vuestro supervisor directo después de completar cada sesión de formación.

El primer correo electrónico de formación se enviará el [MM/DD]. Mientras tanto, podéis consultar las políticas actualizadas para obtener más información sobre esta iniciativa.

Si tenéis alguna pregunta sobre esto, poneos en contacto conmigo.

[FIRMA DE CORREO ELECTRÓNICO]

3

Asunto: Problema de ciberseguridad principal n.º 1: Contraseñas+

¡Hola, equipo!

Esta es la primera sesión de nuestra serie de cursos del Programa de preparación cibernética.

Problema de ciberseguridad principal n.º 1: contraseñas+

Una contraseña es una puerta a una red, a un individuo o a una organización. Usamos cientos de contraseñas y dispositivos conectados en nuestra vida profesional y personal, y cada uno de ellos es una puerta de acceso a nuestra empresa. Una contraseña débil es como dejar la puerta abierta.

Cada una de nuestras contraseñas es un guardián de la información y de los sistemas importantes en los que confiamos y de los que somos responsables. No podemos permitir que sean blancos fáciles.

La primera línea de defensa contra los piratas informáticos oportunistas es una contraseña difícil de descifrar. Crear una contraseña segura solo requiere unos segundos y es algo que todo empleado de [NOMBRE DE LA ORGANIZACIÓN] debe hacer para ayudar a mantener nuestros datos lo más seguros posible.

A continuación se ofrece un breve curso sobre cómo crear contraseñas seguras que puedas recordar y usar fácilmente:

[ENLACE]

También hemos actualizado las políticas de nuestra empresa sobre contraseñas, que se aplican a todos los empleados y personal subcontratado de [ORGANIZACIÓN].

Si tienes alguna pregunta sobre este curso o cómo usar y administrar tus contraseñas, no dudes en comunicarte conmigo directamente.

[FIRMA DE CORREO ELECTRÓNICO]

4

Asunto: Problema de ciberseguridad principal n.º 1: Actualizaciones de software

¡Hola, equipo!

Esta es la segunda sesión de nuestra serie de cursos del Programa de preparación cibernética.

Problema de ciberseguridad principal n.º 2: actualizaciones de software

Probablemente estés familiarizado con esas notificaciones emergentes que te indican que hay una actualización de software disponible para tu ordenador, portátil, tableta o dispositivo móvil. Aunque puede resultar tentador hacer clic en "Recordármelo más tarde", esta no es una buena idea. Las actualizaciones de software reparan importantes brechas de seguridad y corrigen errores críticos que se han identificado, y deben instalarse de inmediato.

No instalar estas actualizaciones deja la puerta abierta a vulnerabilidades de seguridad conocidas que los ciberdelincuentes pueden utilizar y utilizan para entrar y perpetrar un ataque. El infame ataque de ransomware WannaCry se aprovechó de un fallo de seguridad identificado en el sistema operativo Windows que ya se había solucionado en una actualización dos meses antes. Aunque el ataque solo afectó a aquellos que no habían instalado la actualización, en solo 24 horas más de 230.0000 sistemas se vieron comprometidos y causaron daños globales por valor de 4000 millones de dólares.

La instalación de actualizaciones puede eliminar estos puntos de fácil acceso y proteger de los ataques de malware y ransomware. Afortunadamente, las actualizaciones de software son fáciles de realizar.

La mayoría de los sistemas operativos y software se pueden configurar para que se actualicen automáticamente, lo que puede automatizar la instalación de actualizaciones y minimizar la interrupción de tu trabajo. Activar la actualización automática de aplicaciones, sistemas y dispositivos solo requiere unos minutos, así que hazlo lo antes posible.

Al igual que hicimos con las contraseñas, también hemos revisado las políticas de nuestra empresa en torno a las actualizaciones de software. Estos estándares se aplican a todos los empleados y personal subcontratado de [[ORGANIZACIÓN]].

El PDF con la lista de comprobación de actualización de software adjunto ofrece instrucciones paso a paso y enlaces para simplificar esta tarea y lo puedes leer aquí [ENLACE].

Ten en cuenta que cumplir la política y completar el PDF de lista de comprobación de actualización de software es *obligatorio* para todos los empleados de [ORGANIZACIÓN]. Solo tardarás entre 10 y 15 minutos en completar esta lista de comprobación y debes hacerlo antes del [MM/DD]. Asegúrate de informar a tu supervisor una vez que hayas completado esta lista de comprobación.

Si tienes alguna pregunta sobre este curso o sobre cómo usar y administrar las actualizaciones de software, no dudes en comunicarte conmigo directamente.

[FIRMA DE CORREO ELECTRÓNICO]

5

Asunto: Problema de ciberseguridad principal n.º 3: Phishing

¡Hola, equipo!

¿Listo para la tercera sesión de nuestra serie de cursos del Programa de preparación cibernética?

Problema de ciberseguridad principal n.º 3: phishing

El phishing es uno de los ciberataques más utilizados. Cualquiera que tenga una cuenta de correo electrónico o un smartphone puede recibir un mensaje de texto o correo electrónico de phishing. Los ataques de phishing utilizan mensajes engañosos para obtener información confidencial o acceder a una red. Estos mensajes intentan engañar a las personas para que hagan clic en un enlace, descarguen un archivo adjunto en el mensaje o incluso proporcionen directamente información confidencial, como datos bancarios.

La mayoría de nosotros sabemos que el príncipe nigeriano que envía un correo electrónico solicitando una transferencia bancaria de 5000 dólares a su cuenta bancaria es una estafa. Pero las estafas de phishing a menudo son sofisticada y difíciles de detectar si no sabemos qué buscar. Estos mensajes aparentan ser comunicaciones reales que una persona puede recibir legítimamente.

De hecho, 9 de cada 10 ciberataques comienzan con phishing porque los atacantes son expertos en estos ataques. Aunque los métodos que utilizan los estafadores para lanzar ataques de phishing siempre están evolucionando, la mayoría de los mensajes de phishing utilizan varios trucos que puedes aprender a detectar para no dejar que te engañen.

Mira este breve videoclip para aprender algunos trucos para detectar el "phishing" en tus mensajes. [ENLACE DE VÍDEO]

Además, consulta otros trucos para detectar un intento de phishing [AQUÍ].

Si tienes alguna pregunta sobre este curso o sobre cómo usar y administrar las actualizaciones de software, no dudes en comunicarte conmigo directamente.

[FIRMA DE CORREO ELECTRÓNICO]

6

Asunto: Problema de ciberseguridad principal n.º 4: medios extraíbles y transferencia segura de archivos

¡Hola, equipo!

Hoy explicamos el último tema principal de ciberseguridad en nuestra serie de cursos del Programa de preparación cibernética.

Problema de ciberseguridad principal n.º 4: almacenamiento e intercambio de datos

Los USB son una forma fácil y popular de almacenar y transportar archivos, pero también son blancos fáciles para el software malintencionado.

Los piratas informáticos pueden infectar los USB con software malicioso, como virus, spyware, etc., que puede causar daños irrevocables. Alguien que encuentre un USB "perdido" en el parking podría conectarlo a su ordenador para ver qué contiene y devolvérselo al propietario, sin conocer el riesgo antes de que sea demasiado tarde. Los USB no son el único tipo de dispositivo de medios extraíbles; también pueden incluir:

- Discos ópticos (discos Blu-Ray, DVD, CD-ROM)
- Tarjetas de memoria (tarjeta Compact Flash, tarjeta Secure Digital, stick de memoria)
- Discos Zip/Disquetes
- Unidades flash USB
- Discos duros externos (DE, EIDE, SCSSI y SSD)
- Cámaras digitales
- Smartphones
- Otros dispositivos externos/acoplables que contienen funciones de unidades multimedia extraíbles

Hemos actualizado nuestra política empresarial sobre almacenamiento e intercambio de datos, que se aplicará a todos los empleados y personal subcontratado de [ORGANIZACIÓN]:

Si tienes alguna pregunta sobre este curso o sobre cómo usar y administrar las actualizaciones de software, no dudes en comunicarte conmigo directamente.

La próxima semana hablaremos de nuestro nuevo plan de respuesta a incidentes, que nos ayudará a prepararnos y responder a eventos y problemas de ciberseguridad que puedan ocurrir.

[FIRMA DE CORREO ELECTRÓNICO]

7

Asunto: Nuestro plan de continuidad del negocio

¡Hola, equipo!

Hoy vamos a hablar de nuestro plan de continuidad del negocio.

Este plan servirá como un hoja de ruta para nuestra empresa en su conjunto y para que cada persona determine qué hacer y cómo actuar cuando ocurra un problema cibernético o de seguridad.

Las prácticas de higiene cibernética que hemos aprendido durante esta formación y nuestras nuevas políticas de preparación cibernética contribuyen en gran medida a reducir el riesgo de sufrir una vulneración de seguridad. Pero incluso con las mejores medidas implementadas, es importante asumir que probablemente tendremos que lidiar con un incidente de seguridad en algún momento.

Nuestro plan de continuidad del negocio nos prepara para responder, resolver y aprender rápidamente de cada problema que surja. Una crisis puede ser caótica y estresante, pero tener un plan paso a paso garantiza que nuestra respuesta a un ataque sea estratégica y efectiva en lugar de reactiva o inútil.

Hay tres elementos principales para la continuidad de nuestro negocio:

Prepararse

- ✓ Asegúrate siempre de mantener las copias de seguridad actualizadas y sincronizar las cuentas en la nube
- ✓ Mantente siempre alerta ante posibles actividades extrañas o sospechosas

Responder

- ✓ Contacta siempre con [LÍDER EN CIBERSEGURIDAD O CONTACTO DE TI] si detectas algo extraño o sospechoso (por ejemplo, el ordenador se bloquea después de abrir un archivo).
- ✓ Deja de usarlo inmediatamente y desconecta el dispositivo de la red

Recuperarse

- ✓ Notifica el problema a todas las partes afectadas
- ✓ Restablece todas las contraseñas e identificadores
- ✓ Reinstala el software, las cuentas sincronizadas y las copias de seguridad de datos según sea necesario

Hemos actualizado nuestro manual de empresa con este plan de continuidad del negocio. Todos los empleados *y personal subcontratado* de [[ORGANIZACIÓN]] deben consultar y usar este plan, al que puedes acceder aquí [ENLACE].

Si tienes alguna pregunta sobre nuestro plan de continuidad del negocio, no dudes en comunicarte conmigo directamente. La próxima semana, haremos un resumen rápido de lo que hemos aprendido durante este programa y luego [ORGANIZACIÓN] recibirá oficialmente la certificación de preparación cibernética.

[FIRMA DE CORREO ELECTRÓNICO]

8

Asunto: Resumen de preparación cibernética

¡Hola, equipo!

¡Ya hemos completado la serie de cursos del Programa de preparación cibernética! Dediquemos unos minutos a repasar rápidamente lo que hemos aprendido en nuestro viaje hacia la preparación cibernética.

El vídeo sobre los cuatro problemas de ciberseguridad principales

Vídeo del plan de continuidad del negocio

Como siempre, no dudes en ponerte en contacto conmigo directamente si tienes alguna pregunta.

[FIRMA DE CORREO ELECTRÓNICO]

Cuatro módulos básicos de formación:

- **Contraseñas+**
- **Actualizaciones de software**
- **Concienciación sobre el phishing**
- **Almacenamiento e intercambio seguros**
- **Plan de continuidad del negocio**

PowerPoint de formación

- **Plantilla de formación de CRI**

Recursos de formación que se pueden compartir:

- Carteles de CRI: ¿Busca una forma de animar la oficina? ¿Quiere inspirar a su equipo? Examine nuestra colección de carteles, diseños gráficos e infografías sobre preparación cibernética que puede descargar y compartir.
- Guías y consejos de CRI: Una serie de guías para que aprenda más sobre la autenticación multifactor, las relaciones con proveedores externos y otros temas.
- Tarjeta de consejos de phishing de CISA: Consulte este recurso de CISA fácil de compartir con ejemplos y consejos para empleados: Phishing 508 compliant 508 compliant.pdf (cisa.gov)
- Vídeo de formación sobre phishing del Centro de confianza de Mastercard: Comparta este video del Centro de confianza de Mastercard para formar a los empleados sobre las prácticas recomendadas para evitar el phishing: https://youtu.be/CVJiZIjdOOE