SANS SECURITY AWARENESS

Guía de implementación de concientización para la seguridad:
Cómo trabajar desde casa de forma segura

Resumen ejecutivo

Como consecuencia del Coronavirus, muchas organizaciones están implementando el teletrabajo para sus empleados. Esto puede ser un desafío para las organizaciones que no cuentan con las políticas, la tecnología y la capacitación para que su personal trabaje remotamente de forma segura. Asimismo, muchos empleados pueden no estar familiarizados o no sentirse cómodos con la idea de trabajar desde sus hogares. El objetivo de esta guía es permitirle entrenar rápidamente a esas personas para que estén lo más seguras posible. Si tiene preguntas sobre cómo usar esta guía, escríbanos a support@sans.org.

Dado que es muy probable que su personal esté atravesando un momento de cambios y estrés, y que su organización posiblemente tenga limitaciones de tiempo y recursos, el propósito de esta guía es lograr que la capacitación sea lo más simple posible. Le recomendamos que se centre especialmente en los riesgos más significativos que tendrán un mayor impacto, los cuales describiremos a continuación. Piense en ellos como el punto de partida. Si hay riesgos o temas adicionales que desea agregar, no dude en incorporarlos. Tenga en cuenta que, cuantos más procesos, conductas o tecnologías le exija a su personal, será menos probable que logren implementarlos todos.

Cómo usar esta guía

Le recomendamos que, como primer paso, lea el contenido de esta guía y revise los enlaces a los diferentes materiales que se proporcionan para saber lo que tiene a su disposición. Verá que para cada riesgo ofrecemos una variedad de materiales que puede usar para involucrar y capacitar al personal de su organización. Esto le permitirá seleccionar las modalidades que considere que se adaptarán de forma más eficaz a sus necesidades y cultura. Una vez que haya terminado de leer este documento, lea la plantilla de comunicaciones y la hoja informativa complementarias que se incluyen en este kit, a fin de comprender mejor lo que se está intentando lograr. Una vez que haya evaluado la documentación, hay dos grupos clave con los que deberá coordinarse.

1. **Equipo de seguridad**: trabaje con su equipo de seguridad para comprender mejor los riesgos que deberá afrontar. En esta guía, hemos identificado los que creemos que son los riesgos principales y más comunes que presenta el teletrabajo, aunque los suyos pueden ser distintos. A modo de advertencia, tenga en cuenta que un error común que cometen los equipos de seguridad es intentar gestionar todos los riesgos y abrumar a las personas con numerosas políticas y requisitos. Intente limitar los riesgos que abordará a la menor cantidad posible. Una vez que haya identificado y priorizado los riesgos, confirme las conductas necesarias para manejarlos. Como se mencionó antes, si su organización

no tiene el tiempo o los recursos para esta tarea, utilice la información que se indica a continuación.

2. **Comunicaciones**: una vez que haya identificado los principales riesgos humanos y las conductas clave para manejarlos, trabaje con su equipo de comunicaciones para involucrar y capacitar a su personal en dichas conductas. Los programas más eficaces para la concientización en seguridad tienen una sólida relación con sus equipos de comunicaciones. De ser posible, analice si puede incorporar a un miembro del equipo de comunicaciones en su equipo de seguridad. Cuando se comunique con su personal, un argumento efectivo que puede usar para involucrarlos es señalar que esta capacitación no solo les dará seguridad en el trabajo, sino que también les permitirá crear un hogar ciberseguro, lo que los protegerá a ellos mismos y a sus familias.

En definitiva, mediante la colaboración con estos dos grupos, estará motivando a su personal y simplificando al máximo la seguridad: los dos elementos clave para conseguir un cambio de conducta. Incluso, le sugerimos que cree una junta de asesores con personal clave, cuyas observaciones y opiniones necesitará para implementar el programa. Además de los equipos de seguridad y comunicaciones, otros departamentos con los que puede coordinarse y trabajar en conjunto incluyen el de Recursos Humanos y Asuntos Legales.

Paquete de descarga digital MGT433

SANS Institute ofrece el curso de capacitación de dos días MGT433: Cómo crear, mantener y medir un programa de concientización en seguridad de alto impacto. Esta clase intensiva proporciona toda la teoría, las aptitudes, el marco de trabajo y los recursos necesarios para crear un programa de concientización de alto impacto, lo que le permite manejar y medir de forma eficaz el riesgo humano. Como parte de esta guía, le brindamos acceso gratuito al Paquete de descarga digital del curso con plantillas y recursos de planificación. Aunque muy probablemente vayan más allá de las necesidades de esta iniciativa, estos materiales pueden ser valiosos para organizaciones más grandes o implementaciones más complejas.

Responda a las preguntas del personal

Además de comunicarse con su personal y de brindarles capacitación, es sumamente recomendable que implemente algún tipo de tecnología o foro en el que pueda responder a las preguntas de los empleados, preferentemente en tiempo real. Esto puede incluir un alias de correo electrónico específico, un canal de chat de Skype o Slack, o bien algún tipo de foro en línea, como Yammer. Otra idea es organizar un webcast sobre seguridad que pueda repetir varias veces por semana, de manera que las personas puedan elegir un momento que les resulte conveniente y participar en un evento en vivo y, tal vez, hacer preguntas. El objetivo que se intenta alcanzar es lograr que la seguridad sea lo más accesible posible y resolver dudas. Esta es una excelente oportunidad para involucrar a su personal y acercarlos a los conceptos de la seguridad, le recomendamos aprovecharla al máximo.

Tenga en cuenta que, para que esto sea eficaz, debe designar a un recurso que modere los canales de seguridad y responda las consultas de forma activa.

Riesgos y materiales de capacitación

Hemos identificado tres riesgos principales que debería gestionar para su personal remoto. Estos son el punto de partida y, probablemente, los que le resultarán más útiles. Cada uno de los siguientes riesgos tiene enlaces a varios recursos que le ayudarán a comunicar el tema y a brindar capacitación sobre él. Ofrecemos diversos materiales de comunicación, de manera que pueda seleccionar los que generen un mayor impacto en su cultura. Además, casi todos los materiales están disponibles en varios idiomas. Si todo esto le resulta abrumador y cuenta con un tiempo limitado, le recomendamos que simplemente use e implemente los dos documentos que se indican a continuación.

1. Hoja informativa sobre cómo trabajar desde casa de forma segura (incluida en su kit de implementación).
2. Video sobre cómo crear un hogar ciberseguro (inglés), también disponible en otros idiomas aquí.

Ingeniería social

Uno de los riesgos más importantes que deberán enfrentar los trabajadores remotos, especialmente en este momento de cambios drásticos y en un entorno de urgencia, son los ataques de ingeniería social. La ingeniería social es un ataque psicológico en el que los atacantes engañan o embaucan a sus víctimas para que cometan un error, lo que resulta más fácil durante un momento de cambios y confusión. La clave es capacitar a las personas respecto de qué es la ingeniería social, cómo detectar los indicadores más comunes de un ataque de ingeniería social y qué deben hacer cuando lo identifican. Asegúrese de no centrarse únicamente en los ataques de phishing de correo electrónico, también incluya otros métodos, como las llamadas telefónicas, los mensajes de texto, las redes sociales o las noticias falsas. Puede encontrar los materiales necesarios para capacitar y reforzar sobre este tema en nuestra carpeta Materiales de apoyo sobre Ingeniería social. Además, le compartimos el enlace a dos videos sobre concientización en seguridad de SANS que puede utilizar, disponibles en varios idiomas.

- Ingeniería social (inglés), también disponible en otros idiomas aquí.
- Phishing (inglés), también disponible en otros idiomas aquí.

Contraseñas seguras

Tal como se identificó en el Informe anual de filtraciones de datos de Verizon (DBIR), las contraseñas débiles siguen siendo una de las principales causas de las brechas en seguridad

a nivel mundial. Hay cuatro conductas clave que pueden ayudar a manejar este riesgo, las cuales se indican a continuación. Puede encontrar los materiales necesarios para capacitar y reforzar sobre este tema y estas cuatro conductas clave en nuestra carpeta Contraseñas.

- Frases de acceso (tenga en cuenta que tanto la complejidad de la contraseña como el vencimiento de la contraseña son conceptos del pasado).
- Contraseñas únicas para todas las cuentas
- Administradores de contraseñas
- MFA (Autenticación multifactor). También conocida como autenticación de dos factores o verificación en dos pasos.

Sistemas actualizados

El tercer riesgo implica asegurarse de que cualquier tecnología que use su personal ejecute la última versión del sistema operativo, las aplicaciones y las aplicaciones para dispositivos móviles. Para los trabajadores que usen sus dispositivos personales, puede ser necesario habilitar las actualizaciones automáticas. Puede encontrar los materiales necesarios para capacitar y reforzar sobre este tema en las carpetas Programas maliciosos o Cómo crear un hogar ciberseguro.

Temas adicionales de interés

- **Wi-Fi**: proteja su punto de acceso Wi-Fi. Este tema está comprendido en los materiales de Cómo crear un hogar ciberseguro. Además, puede usar este video sobre cómo crear un hogar ciberseguro (inglés), también disponible en otros idiomas aquí.

- **VPN**: ¿Qué es una VPN y porqué debería usar una? Le recomendamos el boletín OUCH sobre VPN.

- **Trabajar de forma remota**: esto aplica a las personas que trabajan de forma remota en lugares como cafeterías, terminales de aeropuertos u hoteles, NO para aquellos que trabajan desde casa. Evalúe usar nuestro video de capacitación sobre cómo trabajar de forma remota (inglés), también disponible en otros idiomas aquí.

- **Niños e invitados**: a fin de reforzar la idea de que ni familiares ni invitados deberían acceder a los dispositivos destinados al trabajo, evalúe usar el video de capacitación sobre cómo trabajar de forma remota (inglés), también disponible en otros idiomas aquí.

- **Detección y respuesta**: ¿Desea que los trabajadores informen si creen que se produjo un incidente mientras trabajaban desde sus hogares? De ser así, ¿qué desea que informen y cuándo? Esta información está disponible en los materiales de nuestra carpeta Atacado.

Boletines OUCH

Además, evalúe usar los boletines OUCH disponibles públicamente a fin de respaldar su programa. Cada uno de ellos está traducido en más de veinte idiomas. A continuación, se enumeran los boletines OUCH que creemos que complementan mejor su iniciativa de seguridad para el teletrabajo. Puede encontrar todos los boletines en los archivos de boletines OUCH sobre concientización en seguridad en línea.

INFORMACIÓN GENERAL

Four Steps to Staying Secure (Cuatro pasos para estar a salvo)
https://www.sans.org/security-awareness-training/resources/four-simple-steps-staying-secure

Creating a Cybersecure Home (Cómo crear un hogar ciberseguro)
https://www.sans.org/security-awareness-training/ouch-newsletter/2018/creating-cybersecure-home

INGENIERÍA SOCIAL

Social Engineering (Ingeniería social)
https://www.sans.org/security-awareness-training/ouch-newsletter/2017/social-engineering

Messaging / Smishing (Mensajería y smishing)
https://www.sans.org/security-awareness-training/resources/messaging-smishing-attacks

Personalized Scams (Estafas personalizadas)
https://www.sans.org/security-awareness-training/resources/personalized-scams

CEO Fraud (Suplantación del CEO)
https://www.sans.org/security-awareness-training/resources/ceo-fraudbec

Phone Call Attacks / Scams (Ataques y estafas telefónicas)
https://www.sans.org/security-awareness-training/resources/phone-call-attacks-scams

Stop That Phish (Cómo evitar el phishing)
https://www.sans.org/security-awareness-training/resources/stop-phish

Scamming You Through Social Media (Las estafas en redes sociales)
https://www.sans.org/security-awareness-training/resources/scamming-you-through-social-media

CONTRASEÑAS

Making Passwords Simple (Cómo simplificar las contraseñas)
https://www.sans.org/security-awareness-training/resources/making-passwords-simple

Lock Down Your Login (2FA) (Cómo blindar el inicio de sesión (2FA))
https://www.sans.org/security-awareness-training/ouch-newsletter/2017/lock-down-your-login

ADICIONALES
Yes, You Are a Target (Sí, usted es su objetivo)
https://www.sans.org/security-awareness-training/resources/yes-you-are-target

Smart Home Devices (Dispositivos domésticos inteligentes)
https://www.sans.org/security-awareness-training/resources/smart-home-devices

Consejos sencillos

Consejos y trucos que puede compartir en un formato fácil de usar.

- Los pasos más eficaces que puede llevar a cabo para proteger su red inalámbrica doméstica es cambiar la contraseña predeterminada de administrador, habilitar el cifrado WPA2 (acceso Wi-Fi protegido) y usar una contraseña segura para su red inalámbrica.
- Tenga en cuenta todos los dispositivos conectados a su red doméstica, incluidos monitores para bebes, consolas de videojuegos, TV, electrodomésticos e, incluso, su automóvil. Asegúrese de que todos esos dispositivos estén protegidos con una contraseña segura y que ejecuten la última versión del sistema operativo.
- Uno de los métodos más eficaces para proteger su computadora personal es asegurarse de que tanto el sistema operativo como sus aplicaciones estén actualizados con los parches más recientes. Habilite las actualizaciones automáticas siempre que sea posible.
- Por último, el sentido común es su mejor protección. Si un correo, llamada telefónica o mensaje en línea le resulta extraño, sospechoso o demasiado bueno para ser verdad, puede ser un ataque.
- Asegúrese de contar con una contraseña única y distinta para cada una de sus cuentas. ¿No puede recordar todas sus contraseñas o frases de contraseña? Evalúe usar un administrador de contraseñas para almacenarlas de forma segura.
- La verificación en dos pasos es una de las mejores medidas que puede implementar para proteger cualquier cuenta. Con la verificación en dos pasos, se usa tanto una contraseña como un código que recibe en su dispositivo móvil. Algunos ejemplos de servicios que admiten la verificación en dos pasos incluyen Gmail, Dropbox y Twitter.
- El phishing es cuando un atacante intenta con engaños que haga clic en un enlace

malicioso o que abra un archivo adjunto en un correo electrónico. Sospeche de cualquier correo electrónico o mensaje en línea que tenga un carácter de urgencia, errores ortográficos o se dirija a usted como "Estimado cliente".

Métricas

Las métricas de comportamiento son complejas en esta situación, dado que es más complicado medir cómo se comporta la gente en casa. Además, algunas de estas conductas no son específicas del trabajo (como proteger sus dispositivos Wi-Fi). Sin embargo, puede medir el nivel de compromiso. Hemos notado que los temas personales o sensibles como estos pueden involucrar más a las personas y generar más interés que otros temas. Por eso, las métricas como estas pueden ser valiosas.

- **Interacción**: ¿Con qué frecuencia las personas hacen preguntas, publican ideas o solicitan ayuda en cualquiera de los canales o foros de seguridad que está organizando?
- **Simulaciones**: lleve a cabo algún tipo de simulación de ingeniería social, como ataques de phishing, mensajes de texto o llamadas telefónicas.

Para ver una lista más completa de métricas, descargue la Matriz interactiva de métricas de concientización de seguridad del Paquete de descarga digital MGT433.

Licencia

Autor del kit de implementación

Lance Spitzner tiene más de 20 años de experiencia en seguridad, investigación de amenazas cibernéticas, arquitectura de seguridad, concientización y capacitación. Ayudó a liderar los campos del fraude y la inteligencia cibernética con la creación de los "honeynets", además de fundar el Proyecto Honeynet. Como instructor de SANS, desarrolló los cursos de Concientización en seguridad MGT433 y Cultura de seguridad MGT521. Además, Lance ha publicado tres libros sobre seguridad, brindado asesoramiento en más de 25 países y ayudado a más de 350 organizaciones a crear programas de concientización y cultura en seguridad para afrontar el riesgo humano. Lance es un orador frecuente, tuitero serial (@lspitzner) y trabaja en diversos proyectos de seguridad en comunidades. Antes de dedicarse a la seguridad en la información, Spitzner se desempeñó como oficial en la Fuerza de Despliegue Rápido del ejército y obtuvo una Maestría en Administración de Empresas en la Universidad de Illinois.

Acerca del SANS Institute

El SANS Institute se fundó en 1989 como una organización de investigación y educación cooperativa. SANS es el mayor y más confiable proveedor de capacitación y certificación en ciberseguridad para profesionales en instituciones gubernamentales y comerciales de todo el mundo. Los reconocidos instructores de SANS enseñan más de 60 cursos diferentes en más de 200 eventos de capacitación en ciberseguridad, tanto en vivo como en línea. GIAC, una filial de SANS Institute, valida las cualificaciones de cada profesional mediante más de 35 certificaciones técnicas y prácticas en ciberseguridad. El SANS Technology Institute, una subsidiaria independiente autorizada regionalmente, ofrece Maestrías en Ciberseguridad. SANS también ofrece un sinfín de recursos gratuitos a la comunidad de InfoSec, incluidos proyectos de consenso, informes de investigación y boletines. Además, gestiona el sistema

de alerta temprana de Internet: el Internet Storm Center. En el corazón de SANS se encuentran los numerosos profesionales en seguridad, que representan una variedad de organizaciones mundiales, desde corporaciones hasta universidades, que trabajan juntas para ayudar a toda la comunidad de seguridad de la información. (https://www.sans.org)