SANS SECURITY AWARENESS

Guía de implementación de concienciación en seguridad – Trabajar de forma segura desde casa

Resumen

A causa del coronavirus, muchas organizaciones se están adaptando para que sus plantillas puedan trabajar desde casa. Esto puede resultar complicado, ya que muchas organizaciones carecen de las políticas, la tecnología y la formación para proteger el trabajo a distancia. Además, muchos empleados no están acostumbrados o no se sienten cómodos ante la idea de trabajar desde casa. La finalidad de esta guía es ayudarle a formar a estas personas para que se protejan. Si tiene alguna pregunta sobre cómo usar la guía, contacte con nosotros a través de support@sans.org.

Dado que su plantilla probablemente estará sufriendo un gran estrés por los cambios, y su organización tendrá limitaciones de tiempo y recursos, esta guía estratégica se centra en que la formación sea lo más sencilla posible. Le recomendamos que se centre en los riesgos más importantes y con mayor impacto, como describimos a continuación. Considere este contenido un punto de partida. Si hay riesgos o temas adicionales que quiera añadir, le animamos a hacerlo. Pero tenga en cuenta que, cuantas más normas, tecnologías o procedimientos exija a su plantilla, menos probable será que puedan implementarlo todo.

Cómo usar esta guía

Le recomendamos empezar leyendo el material de la guía y revisando los enlaces a los diferentes materiales para hacerse una idea del contenido a su disposición. Observará que, por cada riesgo, incluimos una serie de materiales que puede emplear para interactuar con su plantilla y formar a los empleados. Así podrá seleccionar las modalidades que cree que funcionarán de forma eficaz según sus necesidades. Cuando termine de leer este documento, lea la plantilla de comunicaciones y la hoja de datos que incluye este kit para entender mejor los objetivos que se pretenden lograr. Después de consultar la documentación, hay dos grupos principales con los que deberá coordinarse.

1. **El equipo de seguridad**: Coordínese con su equipo de seguridad para entender mejor los riesgos esenciales que intenta gestionar. En esta guía hemos identificado los que nos parecen los riesgos principales y más comunes para una plantilla que trabaje desde casa, pero en su caso pueden variar. Un error habitual que cometen muchos equipos de seguridad es intentar gestionar todos los riesgos y abrumar a los usuarios con un exceso de políticas y requisitos. Intente limitar los riesgos gestionados a los imprescindibles. Después de identificar y priorizar esos riesgos, confirme las actividades destinadas a gestionarlos. Como ya hemos mencionado, si su organización no tiene tiempo ni recursos para ello, puede basarse en los que hemos documentado a continuación.

2. **Comunicaciones**: Después de identificar los principales riesgos humanos y las actividades esenciales para gestionarlos, colabore con su equipo de comunicaciones para informar a su plantilla. Los programas de concienciación en seguridad más efectivos son los que trabajan de cerca con el equipo de comunicaciones. A ser posible, intente que alguien del equipo de comunicaciones se integre en el de seguridad. Al comunicar información a su plantilla, un gancho eficaz es destacar que no solo estarán protegidos en su trabajo, sino que también protegerán en casa sus propios datos y los de su familia.

En última instancia, al colaborar con ambos grupos, intentará que la seguridad sea lo más sencilla posible para los empleados, al tiempo que los motiva, dos elementos esenciales para una adaptación satisfactoria. Sugerimos crear un comité asesor con las personas cuyos comentarios e ideas necesitará para implementar el programa. Además de sus equipos de seguridad y comunicaciones, otros departamentos con los que conviene colaborar y coordinarse son el de recursos humanos y el legal.

Paquete de descarga digital de MGT433

SANS Institute ofrece el curso de formación de dos días MGT433: How to Build, Maintain and Measure a High-Impact Security Awareness Program (Cómo crear, mantener y evaluar un programa de concienciación en seguridad de alto impacto). Este curso intensivo incluye toda la teoría, las habilidades, el entorno y los recursos necesarios para diseñar un programa de concienciación en seguridad de alto impacto que permita gestionar y evaluar de forma eficaz el riesgo humano. Como complemento a esta guía, ofrecemos acceso gratuito al paquete de descarga digital de plantillas y recursos de planificación de este curso. Aunque en su mayor parte exceden el ámbito de esta iniciativa, son materiales que pueden resultar valiosos para organizaciones grandes o implementaciones complejas.

Responder a las dudas de la plantilla

Además de la comunicación y la formación, recomendamos ofrecer algún tipo de tecnología o foro desde donde se puedan atender las dudas de los usuarios, preferiblemente en tiempo real. Puede consistir en una dirección de correo específica, un canal de Skype o Slack o algún tipo de foro en línea, como los de Yammer. Otra idea es ofrecer un seminario web sobre seguridad y repetirlo varias veces a la semana, para que los usuarios puedan elegir el momento más conveniente para asistir en tiempo real, incluso con la posibilidad de hacer preguntas. El objetivo es que la seguridad sea lo más accesible posible y ayudar a los usuarios a resolver sus dudas. Es una oportunidad fantástica para interactuar con su plantilla y mostrar la cara amable de la seguridad. Aproveche para sacar algo positivo de esta situación. Para que nuestros consejos resulten eficaces, recomendamos destinar recursos a moderar estos canales y responder activamente a las consultas.

Riesgos y materiales de formación

Hemos identificado tres riesgos principales que debe gestionar para que su plantilla trabaje a distancia. Son un punto de partida y probablemente los conceptos más valiosos para usted. Cada uno incluye enlaces a varios recursos de comunicación y formación. Ofrecemos múltiples materiales de comunicación para que seleccione los que considere más eficaces según sus circunstancias. Además, casi todos están disponibles en varios idiomas. Si todo esto resulta abrumador y su tiempo es extremadamente limitado, recomendamos implementar simplemente los dos materiales indicados a continuación.

1. Hoja de datos para trabajar desde casa de forma segura (incluida en el kit de implementación).
2. El vídeo Crear un hogar ciberseguro (en inglés) también está disponible en otros idiomas.

Ingeniería social

Entre los mayores riesgos del teletrabajo, especialmente en estos tiempos de grandes cambios y un entorno de urgencia constante, se encuentran los ataques de ingeniería social. La ingeniería social es un tipo de ataque que consiste en engañar a sus víctimas para que cometan errores, algo que resulta más fácil en momentos de cambios y confusión. La clave es formar a la gente sobre lo que es la ingeniería social, cómo identificar las señales más habituales de estos ataques y qué hacer al detectar uno. No se centre solo en los ataques de phishing por correo, explique también métodos relacionados con las llamadas, los mensajes de texto, las redes sociales o las noticias falsas. Encontrará los materiales para explicar y repasar este tema en la carpeta Materiales de apoyo sobre ingeniería social. Además, puede enlazar estos dos vídeos de concienciación en seguridad de SANS, también disponibles en varios idiomas.

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

Contraseñas seguras

Tal y como se detalla en el informe DBIR anual de Verizon, las contraseñas débiles siguen siendo una de las principales causas de brechas de seguridad a escala mundial. Hay cuatro medidas clave que permiten gestionar el riesgo. Encontrará los materiales para explicar y repasar este tema, así como las cuatro medidas, en la carpeta Contraseñas.

- Frases de acceso (las constraseñas complejas y el vencimiento de contraseñas están obsoletos).
- Contraseñas únicas para cada cuenta
- Gestores de contraseñas

- Autenticación multifactor (también llamada autenticación de doble factor o verificación en dos pasos)

Sistemas actualizados

El tercer riesgo es garantizar que toda la tecnología de su empresa utilice la versión más reciente del sistema operativo, los programas y las aplicaciones para móviles. Quienes usen dispositivos personales tendrán que activar las actualizaciones automáticas. Encontrará los materiales para explicar y repasar este tema en las carpetas Programas maliciosos y Crear un hogar ciberseguro.

Temas adicionales que tener en cuenta

- **Wi-Fi**: Proteja su punto de acceso Wi-Fi. Esto se explica en los materiales de Crear un hogar ciberseguro. Además, puede usar el vídeo Crear un hogar ciberseguro (en inglés), también disponible en otros idiomas.

- **VPN**: Qué es una VPN y por qué debería usarla. Recomendamos el boletín OUCH sobre VPN.

- **Trabajar de forma remota**: Para personas que trabajen a distancia, pero no desde casa. Por ejemplo, en una cafetería, en la terminal del aeropuerto o en un hotel. Use nuestro vídeo de formación Trabajar de forma remota (en inglés), también disponible en otros idiomas.

- **Niños e invitados**: Para reforzar la idea de que los familiares e invitados no deben acceder a los dispositivos de trabajo, puede usar el vídeo de formación Trabajar de forma remota (en inglés), también disponible en otros idiomas.

- **Detección y respuesta**: ¿Quiere que sus empleados informen si creen que ha habido algún incidente mientras trabajan desde casa? De ser así, ¿qué deben denunciar y cuándo? Nuestros materiales sobre ataques lo explican**.**

Boletines OUCH

Además, puede usar los boletines OUCH, disponibles públicamente, como refuerzo para su programa; están traducidos a más de veinte idiomas. A continuación encontrará los boletines OUCH que consideramos más útiles para las iniciativas por un trabajo seguro desde casa. Los encontrará todos en el archivo de boletines de seguridad OUCH, disponible en línea.

RESUMEN

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 (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 (Mensajes 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 de directivos)
https://www.sans.org/security-awareness-training/resources/ceo-fraudbec

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

Stop That Phish (Parar la suplantación)
https://www.sans.org/security-awareness-training/resources/stop-phish

Scamming You Through Social Media (Estafas a través de redes sociales)
https://www.sans.org/security-awareness-training/resources/scamming-you-through-social-media

CONTRASEÑAS

Making Passwords Simple (Contraseñas sencillas)
https://www.sans.org/security-awareness-training/resources/making-passwords-simple

Lock Down Your Login (2FA) [Inicios de sesión seguros (doble factor)]
https://www.sans.org/security-awareness-training/ouch-newsletter/2017/lock-down-your-login

CONTENIDO ADICIONAL

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

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

Consejos rápidos

Trucos y sugerencias que puede compartir en un formato fácil de asimilar.

- Los pasos más efectivos que puede llevar a cabo para proteger su red inalámbrica en casa son cambiar la contraseña de administrador predeterminada, habilitar el cifrado WPA2 y usar una contraseña segura para acceder a la red.
- Sea consciente de todos los dispositivos que se conectan a la red, incluidos monitores de bebés, consolas de videojuegos, televisores, electrodomésticos o incluso coches. Procure que todos tengan una contraseña segura y una versión actualizada del sistema operativo.
- Una de las formas más efectivas de proteger su ordenador en casa es asegurarse de que las aplicaciones y el sistema operativo cuenten con los parches y actualizaciones más recientes. Habilite las actualizaciones automáticas siempre que pueda.
- En última instancia, el sentido común es la mejor protección. Si un correo, mensaje o llamada le resultan extraños, sospechosos o demasiado buenos para ser ciertos, puede ser un ataque.
- Use contraseñas únicas y seguras para cada una de sus cuentas. ¿Le cuesta recordar todas sus contraseñas o frases de acceso? Use un gestor de contraseñas para almacenarlas de forma segura.
- La verificación en dos pasos es una de las mejores medidas para proteger cualquier cuenta. Consiste en pedir una contraseña y un código enviado a un dispositivo móvil o

generado por él. Algunos servicios que la ofrecen son Gmail, Dropbox y Twitter.

- El phishing consiste en que un atacante intenta engañarle para que haga clic en un enlace malintencionado o abra un archivo adjunto de un correo. Sospeche de cualquier correo o mensaje que cree sensación de urgencia, esté mal escrito o se dirija a usted como "Estimado cliente".

Métricas

Las métricas de comportamiento son difíciles de evaluar en esta situación, ya que no es fácil medir cómo se comporta la gente en casa. Además, algunos comportamientos no son específicos del trabajo (como proteger su dispositivo Wi-Fi). No obstante, se puede medir la implicación. Sabemos que los temas personales o emotivos como estos pueden fomentar más interés que otros. Por lo tanto, ese tipo de métricas pueden tener valor.

- **Interacción**: ¿Con qué frecuencia hace la gente preguntas, publica ideas o pide ayuda en alguno de los canales o foros de seguridad que ofrece?
- **Simulaciones**: Lleve a cabo algún tipo de simulaciones de ingeniería social, como ataques de phishing, mensajes de texto o ataques por teléfono.

Para una lista de métricas más completa, descargue la matriz interactiva de métricas de concienciación en seguridad del paquete de descarga digital de MGT433.

Licencia

Autor del kit de implementación

Lance Spitzner tiene más de 20 años de experiencia en investigación de amenazas informáticas, arquitectura de seguridad, concienciación y formación. Fue uno de los pioneros en los campos del engaño y la ciberinteligencia, como creador de las honeynets y fundador del Proyecto Honeynet. Como instructor de SANS, ha desarrollado los cursos MGT433: Security Awareness (Concienciación en seguridad) y MGT521: Security Culture (Cultura de la seguridad). Además, Lance ha publicado tres libros sobre seguridad, ha sido asesor de más de 25 países y ha ayudado a más de 350 organizaciones a crear programas de cultura y concienciación en seguridad para gestionar el riesgo humano. Lance es un ponente asiduo, adicto a Twitter (@lspitzner) y trabaja en varios proyectos colaborativos sobre seguridad. Antes de dedicarse a la seguridad de la información, estuvo en la fuerza de despliegue rápido del ejército estadounidense y estudió un máster en la Universidad de Illinois.

Acerca de SANS Institute

SANS Institute se fundó en 1989 como organización dedicada a la investigación y la formación de carácter cooperativo. SANS es el proveedor más fiable e importante de formación y certificaciones de ciberseguridad para profesionales de organismos públicos e instituciones comerciales de todo el mundo. Los prestigiosos instructores de SANS imparten más de 60 cursos diferentes en más de 200 eventos de formación en ciberseguridad presenciales y en línea. GIAC, organización afiliada a SANS Institute, valida las cualificaciones de los profesionales a través de 35 certificaciones en ciberseguridad de carácter técnico y práctico. SANS Technology Institute, una filial independiente acreditada regionalmente, ofrece titulaciones de máster en ciberseguridad. SANS ofrece una gran cantidad de recursos gratuitos a la comunidad de la seguridad informática, incluidos proyectos de consenso, estudios y boletines; también gestiona el sistema de alerta temprana de Internet: Internet Storm Center. En el núcleo de SANS hay muchos profesionales de la seguridad representando a diversas organizaciones, desde corporaciones hasta universidades, que colaboran para ayudar a toda la comunidad de la seguridad de la información. (https://www.sans.org)