CYBER READINESS
INSTITUTE

Consejos y Directrices de Preparación Cibernética

M La mayoría de las compañías cuentan con directrices que todos los colaboradores están obligados a seguir a cerca de responsabilidades básicas como asistir puntualmente al trabajo, o cómo vestir en la oficina, o cómo solicitar vacaciones. Las directrices básicas sobre preparación cibernética deberían ser incluidas también. Después de todo, la seguridad de sus datos y sistemas tiene un gran impacto en su empresa y sus clientes. Le recomendamos emplear los consejos y directrices que ofrecemos a continuación para instruir a sus colaboradores y hacer responsables a todos los miembros de equipo de la creación de una cultura de preparación cibernética.

Contraseñas

Las contraseñas fuertes son esenciales para mantener la seguridad de sus sistemas y cuentas. Ya sea que usted acceda a sus correos electrónicos de trabajo, extraiga archivos de un disco duro compartido o ingrese en cualquier servicio en línea, la contraseña, o la frase de acceso que usted emplea conlleva una gran importancia. Usted puede incluso añadir otra capa de seguridad con una doble autenticación. La doble autenticación requiere que usted ingrese un código único que es enviado a su teléfono móvil cada vez que usted intenta acceder nuevamente. La doble autenticación crea un vínculo de seguridad importante entre la contraseña y la persona.

Le invitamos a seguir estas directrices para con sus colaboradores:

1. Emplee frases de acceso largas que incluyan caracteres especiales. Por ejemplo, escoja una línea de su show de TV favorito, de una película o de una canción.

2. Nunca use la misma frase de acceso para cuentas personales y cuentas de trabajo, y no comparta su nombre de usuario con nadie, ni siquiera con los miembros del equipo.

3. Utilice la doble autenticación cada vez que le sea posible.

Actualizaciones de Software

Es de suma importancia mantener actualizados todos los softwares y sistemas operativos. Cada actualización publicada por el proveedor de software puede incluir importantes correcciones y parches que protegen de ataques a su software y sistemas. Muchas compañías asignan a una misma persona para que gestione las actualizaciones de todos los computadores, lo que es recomendable. De manera alternativa, usted puede solicitar a cada colaborador que gestione sus propias actualizaciones. De cualquier forma, resulta de suma importancia efectuar las actualizaciones de manera regular.

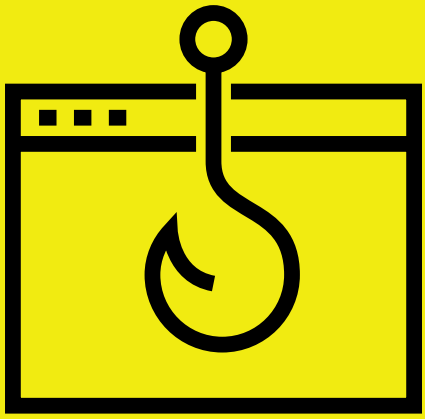
Le recomendamos tomar en cuenta las siguientes directrices relativas a las actualizaciones:

1. Encienda las actualizaciones automáticas en todos sus dispositivos y softwares cuando se presente la opción

2. Actualice con regularidad todos los sistemas operativos, softwares y aplicaciones para computadores, teléfonos y tabletas tan pronto como reciba una notificación que indique que una actualización se encuentra disponible.

3. Actualice todos los softwares y aplicaciones – tanto aquellos emanados de la compañía como aquellos descargados por el colaborador.

El Phishing, o suplantación de identidad



El Phishing, o suplantación de identidad, es una de las cuestiones cibernéticas más comunes y peligrosas hoy en día. Con frecuencia, un correo electrónico de phishing puede aparentar ser un mensaje auténtico y seguro. Pero abrirlo puede resultar en la descarga de virus de software u otorgar a los hackers acceso a sus datos. Todo el mundo recibe correos electrónicos de phishing. Por ello es tan importante saber qué es lo que debemos identificar. La concientización es la mejor defensa contra el phishing.

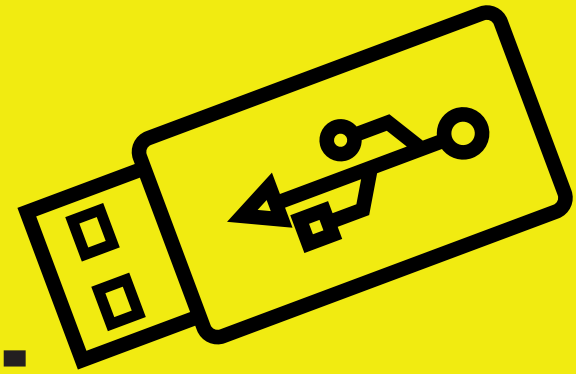
He aquí algunos consejos que le ayudarán:

1. Revise la dirección de correo electrónico del remitente y cualquier otra información que lo identifique, tales como el logo de la compañía, la dirección física y detalles de contacto e intente identificar inconsistencias o señales de que pueda ser fraudulento.

2. Si no está familiarizado con el remitente del correo electrónico, no haga clic en ninguno de los vínculos o descargue ningún adjunto contenido en el mismo

3. Borre cualquier correo electrónico sospechoso e inmediatamente vacíe su papelera.

Unidades USB y Medios Removibles



Las unidades USB son útiles para la transmisión de datos entre computadores, pero también pueden ser utilizadas para transmitir virus y malware. No hay forma de determinar dónde ha estado la unidad, o quién la ha manipulado. La mejor forma de evitar los riesgos con unidades USB y otros medios removibles es evitar usarlos del todo. Sin embargo, establecer una prohibición total del uso de unidades USB puede constituir todo un reto.

Por consiguiente, recomendamos que todos los colaboradores sigan las directrices a continuación:

1. Presente alternativas al uso de unidades USB que sean fáciles de usar, tales como la transmisión de archivos a través de servicios en nube, de manera que las unidades USB sean cada vez menos necesarias.

2. Designe un computador que no esté conectado a la red de la compañía, que pueda ser usado como detector de malware para las unidades USB y para extraer de estas la información necesaria.

3. Más importante aún, use un buen juicio. Si usted no sabe de dónde proviene la unidad, no la conecte.

Respuesta a Incidentes

La preparación cibernética consiste en dar los pasos adecuados para reducir el riesgo, pero también en estar preparados para cuando ocurra un incidente. Contar con un plan de respuesta ante incidentes constituye un paso de vital importancia para estar ciberlistos. Piense en ello como un simulacro de incendio – si una emergencia efectivamente tiene lugar, es importante contar con un plan definido y que todos conozcan el rol que deben desempeñar.

Usted encontrará información adicional sobre la respuesta a incidentes en el Programa de Preparación Cibernética, pero como mínimo, enfóquese en estas tres áreas:

1. **Preparación:** Asegúrese que todos los colaboradores lleven a cabo respaldos regulares de su trabajo y sus datos.

2. **Respuesta:** Si ocurre un ataque u otra cuestión, desconecte inmediatamente el dispositivo afectado de la red de la compañía. Se debe solicitar a todos los empleados que lleven a cabo este paso.

3. **Recuperación:** Restaure los datos perdidos mediante un respaldo, y considere el incidente como una experiencia de aprendizaje para reforzar la importancia de los principios de preparación cibernética como las contraseñas de seguridad, la actualización de softwares, la concientización del phishing y la seguridad de unidades USB.

¿LISTO PARA LLEVAR SUS HABILIDADES AL SIGUIENTE NIVEL?

EXPLORE EL PROGRAMA DE PREPARACIÓN CIBERNÉTICA

El Programa de Preparación Cibernética es un recurso en línea gratuito que establece pasos prácticos que usted puede tomar para evaluar y mejorar su preparación cibernética.
Es fácil de usar y le permite monitorear fácilmente su progreso. Usted puede trabajar a su ritmo. Una vez haya culminado, usted recibirá un Certi icado de Preparación Cibernética y podrá mostrar a sus clientes y proveedores que usted ha tomado los pasos hacia la creación de una cultura de preparación cibernética en toda la organización.

Usted puede saber más en:

https://www.cyberreadinessinstitute.org/es/the-cyber-readiness-program