CYBER READINESS
INSTITUTE

Consejos y directrices de la preparación cibernética

La mayoría de empresas cuentan con directrices que todos los empleados deben seguir sobre responsabilidades básicas como llegar al trabajo a tiempo, qué ropa llevar a la oficina o cómo solicitar las vacaciones. Las directrices sobre preparación cibernética básica también deben estar incluidas. Después de todo, la seguridad de sus datos y sistemas tiene un enorme impacto en su empresa y sus clientes. Le recomendamos que utilice los siguientes consejos y directrices para ayudar a informar a sus empleados y exigir responsabilidades a todos los miembros del equipo para crear una cultura de preparación cibernética.

Contraseñas

Las contraseñas seguras son esenciales para proteger sus sistemas y cuentas. Tanto si accede a correo electrónico del trabajo como si recupera archivos de un disco duro o inicia sesión en algún servicio en línea, la contraseña o la *frase* de contraseña que utilice es importante. Incluso puede añadir otra capa de seguridad con la autenticación de dos factores. Estos dos factores requieren que introduzca un código único que se envía a su dispositivo móvil para cada nuevo inicio de sesión. La autenticación de dos factores crea un importante vínculo de seguridad entre la contraseña y la persona.

Le animamos a que utilice estas directrices para sus empleados:

1. Utilice una frase de contraseña larga que tenga como mínimo 15 caracteres. Por ejemplo, escoja una frase de su programa de televisión, película o canción favorita.

2. Nunca utilice la misma frase de contraseña para cuentas personales y del trabajo, y no comparta sus nombres de usuario y contraseñas con nadie, ni siquiera con los miembros de su equipo.

3. Utilice una autenticación de dos factores siempre que esté disponible.

Acyualiza-cionesde software

Es fundamental mantener actualizados todos los sistemas operativos y software. Cada actualización publicada por el proveedor de software puede incluir correcciones y parches importantes que protegen sus sistemas y software frente a los ataques. Muchas empresas asignan a una persona la gestión de actualizaciones de todos los ordenadores de la empresa, lo cual es preferible. Como alternativa, puede requerir que cada empleado gestione sus propias actualizaciones. En cualquier caso, las actualizaciones periódicas tienen una importancia trascendental.

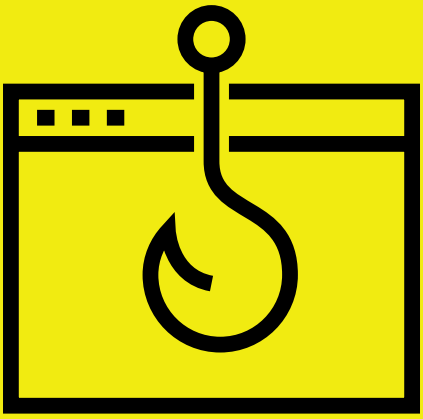
Recomendamos las siguientes directrices para las actualizaciones:

1. Active la función de actualización automática en todos los dispositivos y software siempre que se le ofrezca.

2. Actualice con regularidad todos los sistemas operativos, software y aplicaciones de ordenadores, teléfonos y tabletas en cuanto reciba una notificación que indique que hay una actualización lista.

3. Compruebe periódicamente que todas las actualizaciones están instaladas y que no se ha perdido ninguna notificación.

Phishing



El phishing es uno de los problemas cibernéticos más habituales y más peligrosos de hoy en día. Con frecuencia, un correo electrónico de phishing puede parecer un mensaje real y seguro. Sin embargo, abrirlo puede provocar la descarga de virus de software o brindar acceso a los atacantes a sus datos. Todo el mundo recibe correos electrónicos de phishing. Por eso es importante saber lo que se debe buscar. La concienciación es la mejor defensa contra el phishing.

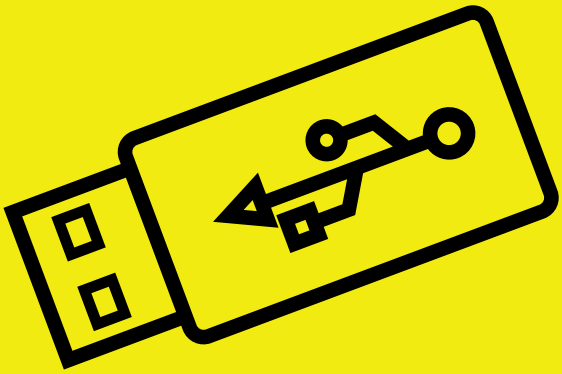
Aquí le mostramos algunos consejos que le ayudarán a:

1. Comprobar la dirección de correo electrónico del remitente y cualquier otra información de identificación, como el logotipo de la empresa, la dirección y los datos de contacto, para ver si hay incoherencias o signos de que pueda ser falsa.

2. Si no está familiarizado con el remitente del correo electrónico, no haga clic en ningún enlace ni descargue ningún archivo adjunto del correo electrónico.

3. No facilitar ninguna información personal en la respuesta.

Unidadees USB Y medios extraíbles



Las unidades USB resultan útiles para compartir archivos entre ordenadores, pero también se pueden utilizar para enviar virus y malware. No existe ninguna forma de saber dónde ha estado la unidad o quién puede haberla comprometido. La mejor manera de evitar riesgos con las unidades USB y otros medios extraíbles es evitar su uso por completo. Sin embargo, prohibir totalmente las unidades USB puede ser un reto.

Por tanto, recomendamos que todos los empleados sigan las directrices siguientes:

1. Presentar alternativas fáciles de usar a las unidades USB, como los servicios de intercambio de archivos basados en la nube, para que las unidades USB no sean necesarias.

2. Nunca aceptar o utilizar una unidad USB de un tercero no verificado.

3. Y lo más importante, utilizar el sentido común. Si no sabe de dónde procede la unidad, no la conecte.

Respuesta a incidentes

La preparación cibernética consiste en tomar las medidas adecuadas para reducir el riesgo,pero también en estar preparado cuando se produzca un incidente. Disponer de un plan de respuesta a incidentes es un paso fundamental para la preparación cibernética. Piense en ello como en un simulacro de incendio: si se produce una emergencia, es importante contar con un plan en el que todos sepan su función.

Encontrará más información sobre la respuesta a incidentes en el Programa de Preparación Cibernética, pero como mínimo, céntrese en estas tres áreas:

1. **Preparación:** asegúrese de que todos los empleados realicen copias de seguridad periódicas de su trabajo y sus datos.

2. **Respuesta:** si se produce un ataque o un problema, desconecte de inmediato el dispositivo afectado de la red de la empresa. Se debe exigir a todos los empleados que den este paso.

3. **Recuperación:** restaure los datos perdidos desde una copia de seguridad, notifique a todas las partes afectadas y restablezca el id. y la contraseña del dispositivo afectado.

¿LISTO PARA LLEVAR SUS HABILIDADES AL SIGUIENTE NIVEL?

EXPLORE EL PROGRAMA DE PREPARACIÓN CIBERNÉTICA

El Programa de Preparación Cibernética es un recurso gratuito y disponible en línea que describe los pasos prácticos que puede seguir para evaluar y mejorar su preparación cibernética. Utilizarlo y realizar un seguimiento de su progreso es sencillo. Puede trabajar a su ritmo. Una vez completado, recibirá un Certificado de preparación cibernética para mostrar a los clientes y proveedores que ha tomado medidas para crear una cultura de preparación cibernética en toda su organización.

Más información:

BeCyberReady.com