Consejos para las compras navideñas para minoristas

La temporada de compras navideñas está en pleno apogeo y los minoristas de todo el mundo se están preparando para la oleada de pedidos que llegan en las semanas previas a las fiestas. A la luz de los retos a los que se enfrentan los minoristas, **es fundamental priorizar los riesgos de ciberseguridad.**

A continuación se presentan consejos sobre preparación cibernética que los minoristas deben seguir para **mantenerse seguros** mientras compran en línea.

Consejo nº 1 Mantener el software actualizado

- Active las **actualizaciones automáticas pa**ra todo el software.
- Cada actualización contiene las últimas correcciones y parches, que pueden protegerle contra amenazas potencialmente peligrosas.
- **Reiniciar el ordenador** también es otra forma de asegurar que los parches se instalen.

Consejo nº 2 Definir sus políticas de ciberseguridad

- **Forme a todos sus empleados** en sus políticas de ciberseguridad.
- Muestre a los empleados la importancia de la ciberseguridad y el papel que tiene en su vida personal y profesional.
- **Inscríbase en nuestro programa gratuito de preparación cibernética** y acceda a otros recursos de CRI para desarrollar buenos hábitos de preparación cibernética.

Consejo nº 3 Deshacerse de los USB

- Aunque las unidades USB son útiles para transferir archivos entre ordenadores, también pueden utilizarse para propagar **virus y malware.**
- Configure un **ordenador de red no perteneciente a la empresa** que pueda utilizarse para analizar unidades USB en busca de malware y eliminar la información de las unidades.
- Adopte un **sistema de intercambio de archivos en línea o en la nube** que tenga acceso protegido para no tener que usar un USB.

Consejo nº 4 Estar atento al phishing durante las fiestas

- Permanezca atento a las estafas de phishing y a los mensajes maliciosos que intentan aprovecharse de los compradores ocupados y distraídos.
- Compruebe la dirección de correo electrónico del remitente y revise los correos electrónicos cuidadosamente para asegurarse de que el remitente es legítimo. Si parece demasiado bueno para ser verdad, probablemente lo sea.
- Nunca haga clic en los enlaces, descargue archivos adjuntos ni responda con información a remitentes desconocidos. Aunque "conozca" a la persona, siempre es bueno enviarle un mensaje o llamarle para verificarlo antes de actuar.

Consejo nº 5 Mantener las contraseñas seguras

- Asegúrese de que sus frases de acceso sean **seguras y únicas** para cada cuenta.
- Siempre que sea posible, active la **autenticación multifactor (MFA)** en todas sus cuentas.
- Nunca revele sus contraseñas a nadie y **cámbielas siempre después de viajes** o actividades en las que haya iniciado sesión en una cuenta en el dispositivo de otra persona.