CYBER READINESS
INSTITUTE

Felices y tranquilas fiestas

Consejos de preparación cibernética para minoristas durante las fiestas

La temporada de compras navideñas está en pleno apogeo pero, como tantas otras actividades habituales, **este año las compras son diferentes debido a la pandemia de la COVID-19.**

Ahora más que nunca, los consumidores apuestan por las compras en línea. Según McKinsey, se espera que entre el 30 y el 60 por ciento de los consumidores de todo el mundo compren en línea en lugar de en tiendas físicas durante las fiestas. Los minoristas han tenido que responder facilitando a los consumidores las compras en línea y estableciendo nuevas formas para que los compradores reciban sus artículos. Para muchos minoristas, esta realidad les ha llevado a contratar servicios de entregas, lo que significa que los minoristas están compartiendo información de los clientes con terceros. Todo el proceso de compra, desde el inicio al fin, se basa cada vez más en la transferencia de información entre usted y sus clientes, que utilizan ordenadores y smartphones. La avanzada tecnología actual ha hecho posible que los minoristas, incluso los más pequeños, trasladen rápidamente gran parte de su negocio a una plataforma digital. Es algo muy positivo para abordar los desafíos comerciales que se han incrementado debido a la pandemia.

La parte negativa es que los delincuentes también se han pasado al mundo digital. Los ciberdelincuentes saben que cada vez más personas compran en línea y que los minoristas recopilan y comparten información más valiosa sobre sus clientes, incluidos números de tarjetas de crédito, direcciones e identificación con fotografías para recoger pedidos. Se ha producido un enorme aumento en los ataques de phishing por correo electrónico y mensajes de texto (intentos de engañarle para que haga clic en un enlace o envíe información), así como en los ataques de ransomware con los que los delincuentes retienen su sistema informático y sus datos como rehenes hasta que reciben un pago. El FBI ha informado de un aumento del 400 por ciento en las quejas sobre ciberataques desde antes de la COVID-19. Por su parte, la Interpol ha registrado una “tasa alarmante de ciberataques” dirigidos a empresas de todos los tamaños, Gobiernos e infraestructuras críticas durante la pandemia.

Sabemos que es una época del año de gran actividad y que usted se centra en atender a sus clientes. Somos conscientes de que puede estar contratando trabajadores temporales o empezando a trabajar con nuevos servicios y socios de entregas. Pero los delincuentes también lo saben y cuentan con que usted se distraiga y descuide su nivel de preparación cibernética. Por desgracia, el 60% de las pymes quiebran en los 6 meses posteriores a sufrir un incidente cibernético grave, según la National Cyber Security Alliance.

guide@cyberreadinessinstitute.com

Aunque piense que su empresa es demasiado pequeña para ser objetivo de ataques, puede ser una puerta de entrada fácil a un objetivo más grande deseado.

A continuación, se ofrecen algunos consejos que le ayudarán a estar preparado para la cibernética en la temporada de compras navideñas:

Qué hacer

- Actualice inmediatamente sus contraseñas con 15 caracteres: usar una frase de contraseña puede hacer que sea más fácil de recordar (por ejemplo, la letra de una canción, una frase de un libro)
- Active las actualizaciones automáticas para todo el software
- Utilice la autenticación multifactor siempre que esté disponible
- Asegúrese de que se realizan las copias de seguridad de sus ordenadores y sus datos en una red separada y pruebe esa copia de seguridad de forma habitual
- Aplique ciberpolíticas claras que se comuniquen a todos los empleados
- Forme a los empleados sobre cómo recibir y procesar pedidos en línea de forma segura

Qué evitar

- No haga clic en enlaces y nunca facilite información financiera por correo electrónico
- No comparta sus contraseñas o credenciales de inicio de sesión
- No deje ningún ordenador desatendido y/o desbloqueado
- No suponga que los terceros con los que trabaja están preparados para el ciberespacio (por ejemplo, servicios de entrega, procesadores de pagos, pequeños proveedores)

Recuerde que el comportamiento humano es fundamental para evitar un ciberataque.

Asegúrese de que todos sus empleados y trabajadores temporales hayan recibido formación sobre sus políticas de ciberseguridad, que conozcan su importancia y la función que desempeñan en ella. Ayúdeles a desarrollar buenos hábitos para estar preparados para la cibernética. Para obtener más detalles, regístrese en el Programa de preparación cibernética y consulte nuestras **otras guías** para desarrollar buenos hábitos de preparación cibernética.

Acerca del Cyber Readiness Institute

El Cyber Readiness Institute es una iniciativa sin fines de lucro que reúne a líderes empresariales de todos los sectores y zonas geográficas para compartir recursos y conocimientos que impulsan el desarrollo de herramientas de ciberseguridad gratuitas para las pequeñas (pymes). Explore los elementos básicos de una buena ciberseguridad con nuestro Kit básico o cree una cultura de preparación cibernética en su organización con el Programa de Preparación Cibernética autodirigido y disponible en línea. Nuestras guías sobre Recursos de trabajo remoto y Lugar de trabajo híbrido ofrecen consejos oportunos para abordar los cambiantes retos cibernéticos de hoy en día. Para obtener más información, visite **www.BeCyberReady.com**.

guide@cyberreadinessinstitute.com