CYBER READINESS
INSTITUTE

¡Felices fiestas! Consejos para mantener la ciberseguridad durante las fiestas

En la época navideña, tanto las empresas como los consumidores corren el riesgo de sufrir ciberataques. Muchas organizaciones gubernamentales, como el FBI, la Agencia de Seguridad de Infraestructuras Críticas (CISA) y el Centro Nacional de Ciberseguridad de Reino Unido, han publicado una guía sobre las mejores formas de mantenerse seguro durante estas fiestas. El Cyber Readiness Institute (CRI) ha reunido los aspectos más destacados de estos avisos en una guía navideña de dos partes para consumidores y minoristas.

Consumidores

Tenga en cuenta que los piratas informáticos siempre buscan las formas más eficientes de comunicarse con usted.

El phishing (o smishing) navideño a través de mensajes de texto (SMS) casi se ha duplicado desde el año pasado, según un informe publicado por Proofpoint.

Los piratas informáticos envían mensajes de texto y correos electrónicos **imitando notificaciones de entrega**, notificaciones de seguimiento u ofertas navideñas.

Prácticas recomendadas:

- Comprobar los dispositivos: utilice contraseñas o frases de acceso seguras de al menos 15 caracteres, actualice el software y active la autenticación multifactor.
- Comprar solo a través de fuentes fiables: piense en cómo y dónde está haciendo compras en línea.
- Reconocer las estafas de phishing: no haga clic en enlaces ni descargue archivos adjuntos a menos que esté seguro de dónde provienen. Vuelva a verificar la dirección de correo electrónico del remitente y tenga cuidado con las solicitudes de información personal.
- Nunca proporcione su contraseña, información personal o financiera en respuesta a un correo electrónico o llamada telefónica no solicitados.
- Utilizar métodos seguros para las compras: nunca proporcione información financiera cuando use un wifi público.
- En la medida de lo posible, use una tarjeta de crédito en lugar de una tarjeta de débito y verifique los extractos de su cuenta con frecuencia.

guide@cyberreadinessinstitute.org

Minoristas

Esta es la época más ajetreada del año, no solo para usted, sino también para los piratas informáticos.

Tenga cuidado con los ataques de ransomware. En 2020, muchas empresas conocidas de Estados Unidos sufrieron ataques durante las fiestas, cuando los adversarios sabían que las empresas se apresurarían a cumplir con los pedidos.

Sophos Labs estimó que, en 2020, **el comercio minorista fue el sector más afectado por los ciberataques**. Recuerde que los piratas informáticos pueden intentar atravesar sus sistemas para llegar a sus clientes o proveedores.

Fuentes:

https://www.cisa.gov/news/2021/11/23/cisa-shares-tips-keep-your-personal-data-and-financial-data-safe-holiday-shopping?utm_campaign=wp_the_cybersecurity_202&utm_medium=email&utm_source=newsletter&wpisrc=nl_cybersecurity202

https://www.politico.com/newsletters/national-security-daily/2021/11/22/chinas-missile-turducken-495192

https://us-cert.cisa.gov/ncas/current-activity/2021/11/22/reminder-critical-infrastructure-stay-vigilant-against-threats

https://www.cisa.gov/news/2021/11/22/cisa-and-fbi-urge-organizations-remain-vigilant-ransomware-and-cyber-threats

https://www.proofpoint.com/us/blog/corporate-news/holiday-shopping-themed-mobile-attacks-increase-dramatically

https://us-cert.cisa.gov/ncas/alerts/aa21-243a

https://www.washingtonpost.com/politics/2021/11/24/happy-hacksgiving-officials-warn-surge-cyber-threats/

Prácticas recomendadas:

- Identifique a los trabajadores de tecnología y ciberseguridad que puedan responder rápidamente durante las fiestas si hay un incidente cibernético.
- Advierta al personal de que debe tener cuidado con los correos electrónicos de phishing y otras estafas cibernéticas durante las fiestas.
- Asegúrese de que los parches de software están actualizados en todos los dispositivos de la empresa y en todos los dispositivos personales que utiliza el personal para realizar su trabajo.
- Exija contraseñas seguras, asegurándose de que no se reutilicen en varias cuentas.
- Asegúrese de que todos los sistemas informáticos exigen a los usuarios el uso de la autenticación multifactor, especialmente para el acceso remoto y las cuentas administrativas.
- Recuerde a los empleados que no deben hacer clic en enlaces sospechosos y realice ejercicios de concienciación.
- Revise y, si es necesario, actualice los planes de comunicación y respuesta ante incidentes para enumerar las medidas que tomará la organización si se ve afectada por un incidente.
- Asegúrese de que exista una copia de seguridad de sus sistemas y datos importantes en una ubicación que no esté conectada a su red.

Recordatorio:

Si es víctima de un ciberataque, informe del incidente a la agencia de ciberseguridad de su gobierno, por ejemplo: CISA, FBI, Centro Nacional de Ciberseguridad de Reino Unido, Interpol.

Visite becyberready.com, cisa.gov/shop-safely, us-cert.cisa.gov/ncas/alerts/aa21-243a y stopransomware.gov para obtener más información y conocer las prácticas recomendadas sobre cómo mantenerse seguro durante esta temporada navideña.

CYBER READINESS INSTITUTE