SEA CIBERNÉTICAMENTE INTELIGENTE

#CyberMonth

MES DE CONCIENTIZACIÓN SOBRE SEGURIDAD CIBERNÉTICA DE 2021: PONGA DE SU PARTE. #BECYBERSMART

CIBERNÉTICAMENTE SEGURO EN EL TRABAJO

Los negocios sufren pérdidas económicas significantes cuando un ataque cibernético ocurre. En 2020, se informó de un gran aumento en los ataques cibernéticos dirigidos contra negocios que utilizaban usuarios y contraseñas robadas.[1] Los delincuentes cibernéticos frecuentemente dependen del error humano—cuando los empleados no instalan parches de software o hacen clic en enlaces maliciosos—para obtener acceso a los sistemas. Desde los altos dirigentes hasta el empleado más nuevo, la seguridad cibernética exige la vigilancia de todos para mantener seguros y a salvo a los datos, los clientes y la capital. #BeCyberSmart para conectarse con confianza y promover una cultura de seguridad cibernética en su organización.

CONSEJOS SENCILLOS

- **Trate la información del negocio como si fuera información personal.** La información del negocio suele incluir una mezcla de datos personales y propios. Aunque uno piense en secretos del comercio y cuentas de crédito de la compañía, estos datos también incluyen la información personalmente identificable (PII, por sus siglas en inglés) de los empleados en sus formularios de impuestos y las cuentas de la nómina. No comparta PII con partes desconocidas o a través de redes no aseguradas.
- **No debe ser fácil adivinar sus contraseñas** A medida que la tecnología "inteligente" o impulsada por los datos evoluciona, es importante recordar que las medidas de seguridad solamente funcionan si los empleados las utilizan correctamente. La tecnología inteligente funciona con los datos, lo cual significa que los dispositivos como los teléfonos inteligentes, las computadoras portátiles, las impresoras inalámbricas y otros están constantemente enviando y recibiendo datos para realizar tareas. Tome las medidas de seguridad apropiadas y verifique la configuración correcta de los dispositivos inalámbricos para evitar filtraciones de datos. Para más información sobre la tecnología inteligente, consulte la Tarjeta de consejos sobre el Internet de las cosas.
- **Manténgase al día.** Mantenga su software actualizado a la última versión disponible. Mantenga sus configuraciones de seguridad para que protejan su información, activando las actualizaciones automáticas para no tener que pensar en ellas y configure su software de seguridad para que realice análisis regulares.
- **Las redes sociales forman parte del conjunto de herramientas del fraude.** Al buscar por Google y explorar las páginas de su organización en las redes sociales, los delincuentes cibernéticos pueden recolectar información sobre sus colaboradores y sus proveedores, también como sus departamentos de recursos humanos y finanzas. Los empleados deben evitar compartir demasiado en las redes sociales y no deben realizar negocios oficiales, tramitar pagos o compartir PII en las plataformas de redes sociales. Para más información, lea la Hoja de consejos sobre la seguridad cibernética en redes sociales.

- **Una sola vez es suficiente.** Las filtraciones de datos no suelen ocurrir cuando un delincuente cibernético ha penetrado la infraestructura de una organización. Muchas filtraciones de datos tienen su origen en una sola vulnerabilidad de seguridad, un solo intento de phishing o un solo incidente de exposición accidental. Tenga cuidado de fuentes inusuales, no haga clic en enlaces desconocidos y borre todo mensaje sospechoso después de denunciar o reenviar todos los intentos de phishing a un supervisor, para que se puedan implementar las actualizaciones, alertas o cambios organizacionales que sean necesarios. Para más información sobre las estafas por correo electrónico y de phishing, vea la Hoja de consejos sobre phishing.

SI USTED TRABAJA DESDE CASA

- **Use solamente las herramientas aprobadas.** Solo use el software y las herramientas que su organización ha aprobado para los negocios, incluyendo las herramientas de videoconferencia y colaboración provistas por la compañía para iniciar y programar reuniones.
- **Asegure su reunión.** Adapte las precauciones de seguridad de manera que sean apropiadas para el público destinatario. Planifique lo que se debe hacer si una reunión pública se vea interrumpida. Tome medidas para asegurar que solamente las personas indicadas asistan. a su reunión.
- **Asegure su Información.** Adapte sus precauciones de seguridad de acuerdo con el nivel de confidencialidad de sus datos. Solo comparta los datos necesarios para lograr las metas de su reunión.
- **Asegúrese a sí mismo.** Tome medidas para evitar la divulgación no intencional de su información. Asegure que las redes de su hogar estén aseguradas. Para más información, visite Materiales de referencia sobre el teletrabajo para el empleado en casa.

COMUNÍQUESE CON EL EQUIPO DEL MES DE CONCIENTIZACIÓN SOBRE SEGURIDAD CIBERNÉTICA DE CISA

Muchas gracias por su apoyo y compromiso continuos con el Mes de Concientización sobre Seguridad Cibernética y por ayudar a todos los estadounidenses a mantenerse seguros en Internet. Para aprender más, envíe un mensaje por correo electrónico a nuestro equipo en CyberAwareness@cisa.dhs.gov, o visite www.cisa.gov/cybersecurity-awareness-month o staysafeonline.org/cybersecurity-awareness-month/.

RECURSOS

1. Identity Theft Resource Center. (2021). *2020 Data Breach Report* https://www.idtheftcenter.org/annual-reports/