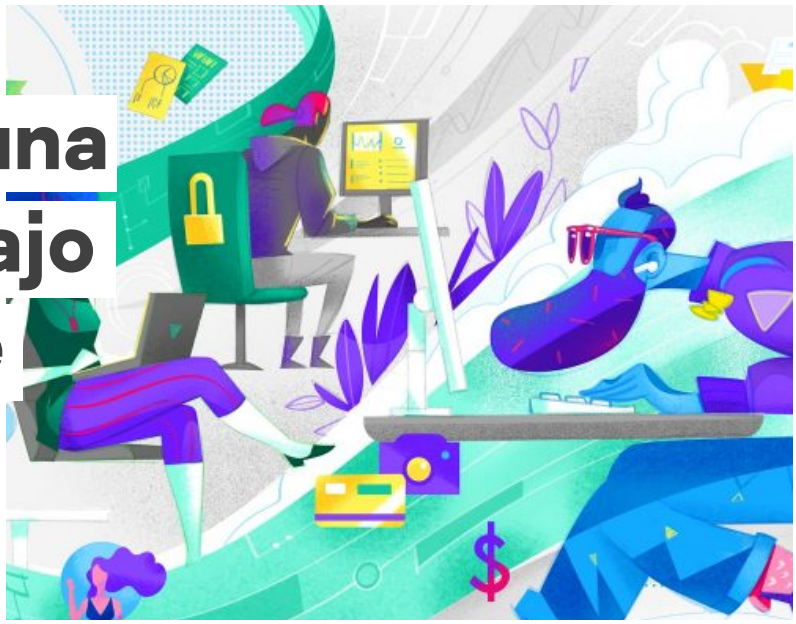
Cómo generar una cultura de trabajo más consciente de la seguridad



Ciberataques: sus empleados pueden ser, tanto su principal defensa como su mayor debilidad. Le explicamos por qué crear una cultura consciente de la ciberseguridad es lo mejor para su empresa.

AUTOR
David Emm

Sus empleados representan uno de los mayores factores de riesgo para la ciberseguridad de su empresa. Puede ofrecerles pláticas, pedirles que hagan pruebas en línea y hasta instalar software en sus computadoras, pero un simple clic distraído en un correo electrónico de phishing podría tener un enorme costo para su empresa. La solución: crear una sólida cultura con conciencia en la ciberseguridad para preservar la seguridad de su empresa.

¿Cuándo fue la última vez que logró motivar a sus empleados sobre temas de ciberseguridad?

Quizás haya realizado una presentación o les haya hecho aprobar una serie de pruebas en línea, pero muy probablemente no le prestaron toda su atención. Hágase esta pregunta: si dijera "sesión de concientización en ciberseguridad", ¿cómo lo tomarían sus empleados? A: estarían interesados y motivados, B: lo verían como una oportunidad para distraerse o C: estarían demasiado preocupados por sus tareas pendientes como para prestar toda su atención. Si respondió A, bien hecho, ya está construyendo una organización con conciencia de ciberseguridad. Si respondió B o C, debe cambiar la dinámica de capacitación de sesiones puntuales a una cultura más integrada en la conciencia sobre la ciberseguridad.

Cultura, no presentaciones

Hace años trabajé en una empresa en la cual una de las principales reglas era: el teléfono nunca debe sonar por cuarta vez. Entonces, todos los empleados, apenas entrábamos a esa oficina, ya sabíamos qué hacer. Y no era necesario que nadie se lo enseñara a los nuevos empleados: podían ver por sí mismos lo que se esperaba de ellos. Simplemente lo hacíamos de forma instintiva. Era parte de nuestra cultura y se volvió un hábito.

> Una fuerte cultura de ciberseguridad no se crea con lecciones aisladas acerca de los peligros del mundo cibernético, se construye con base en participación y hábitos.

Debe considerar las mejores prácticas de ciberseguridad como algo similar a limpiar sus armarios: lo puede hacer una vez, pero inevitablemente tendrá que repetirlo de forma periódica. O para ser más específico, es como instalar un software antivirus en una computadora y nunca actualizarlo. Las culturas sólidas en ciberseguridad no se crean con lecciones aisladas acerca de los peligros del mundo cibernético, se construyen con base en participación y hábitos.

Cómo involucrar a sus empleados y proteger su negocio

En primer lugar, si tiene suficientes fondos, invierta en especialistas en TI. Si designa a alguien para estar a cargo de proteger su negocio, monitorear las amenazas y capacitar a su personal, su empresa estará mejor equipada para hacer frente a los ciberataques. Y asegúrese de que sus equipos de TI cuenten con la capacitación en inteligencia de seguridad y las tecnologías necesarias para detectar y actuar sobre las amenazas.

Pero, ¿qué sucede si la suya es una empresa pequeña o mediana (PyME) con recursos limitados que tal vez tenga pocos o ningún especialista dedicado a TI? Piense en una estrategia paso a paso: acciones pequeñas, pero frecuentes. A medida que sus esfuerzos cobren impulso en la oficina, las personas empezarán a darse cuenta de lo que intenta hacer.

Por ejemplo, un póster en el que se muestren cinco formas de cuidar la ciberseguridad podría lograr llamar la atención si lo coloca en algún lugar transitado, como la cocina o al lado de sus otros pósters de seguridad laboral. O piense en sus procedimientos. Copie la metodología de los correos electrónicos de phishing dirigido (en los que los hackers asumen la identidad de uno de sus empleados) y envíe ataques dirigidos con mayor frecuencia. Asignar a varias personas la responsabilidad de aprobar las transacciones financieras podría bloquear las acciones de los ladrones de identidad. Recompensar a sus colegas y empleados también puede causar un gran efecto. Por ejemplo ¿quién informó acerca de la mayor cantidad de correos electrónicos de phishing? Un cupón de regalo como premio, seguramente logrará que todos quieran informar sobre estas amenazas.

Y, de paso, fomente también otras prácticas de conciencia sobre la seguridad en el trabajo, por ejemplo, interrogue a personas desconocidas que estén en el edificio y evite el desorden digital, como dejar información confidencial en la impresora o en las memorias USB sin ninguna protección.

En definitiva, la forma más efectiva de crear una mejor cultura de ciberseguridad es implementar acciones periódicas. Mi mejor consejo: organice actividades cortas y frecuentes: lecciones, pruebas, simulacros, incluso búsquedas del tesoro o una sala de reuniones transformada en una "sala de escape cibernético" por un día. Brinde a sus empleados, a menudo, una cantidad de información fácil de digerir. Recibirán información en porciones lo suficientemente pequeñas como para integrarlas a sus tareas cotidianas y esto creará la buena base para lograr una sólida cultura de ciberseguridad. ¿El resultado? Mayor protección para su empresa.

Para obtener más consejos sobre conciencia en seguridad y mejores prácticas de ciberseguridad para el entorno laboral, lea una entrevista con Barton Jokinen, el Gerente de seguridad de la información y Cumplimiento normativo de Kaspersky para las Américas.

kaspersky