KnowBe4

Neoway
Uma empresa B3

CASO DE ÉXITO

Neoway y KnowBe4: Crear una Cultura de Seguridad

Neoway es una influyente organización de tecnología B2B en América Latina. Esta organización brasileña es líder del mercado por su plataforma de análisis de macrodatos e IA, y trabaja con clientes de más de 20 sectores industriales, entre los que se incluyen las finanzas, el sector automotor, los bienes de consumo, el petróleo y el gas, y la tecnología, entre otros. La organización ha comprendido la importancia de crear una cultura de la seguridad entre sus empleados.

Una Oportunidad para Hacer que la Seguridad Sea Estratégica

En 2018, Neoway tenía 400 empleados, y su pequeño equipo de Seguridad de la Información dependía del Departamento de Ingeniería. A pesar de tener cientos de trabajadores y estar en una trayectoria de crecimiento, Neoway funcionaba como una empresa emergente en algunos aspectos.

El equipo de Seguridad de la Información sabía que se necesitaban cambios. Al tratarse de una conocida organización de tecnología B2B con una fuerza laboral en crecimiento que, a veces, operaba fuera de su función laboral específica, al equipo de Seguridad de la Información le preocupaba que Neoway pudiera ser objeto de ciberataques, sobre todo, de correos electrónicos de phishing. Se hizo un cambio estratégico: el equipo de Seguridad de la Información pasó de formar parte del equipo de Ingeniería para informar directamente al CEO. Neoway también contrató a profesionales de la seguridad talentosos, como Flavio Costa, Director de Seguridad de la Información (CISO) de la organización, quien podía ayudar a posicionar los programas de seguridad de Neoway como impulsores críticos del negocio. Una de sus primeras tareas fue poner en marcha un programa de capacitación en concientización sobre seguridad.

"KnowBe4... era muy sofisticado, personalizable y asequible; exactamente el tipo de programa que queríamos".

"Aquí tenemos un espíritu emprendedor: si hay que hacer algo, la gente pone manos a la obra, sea cual sea su puesto", afirma Costa. "Eso nos hace muy ágiles y eficientes, pero abre la puerta a cierto riesgo".

Neoway

Industria

Plataforma tecnológica de macrodatos e IA

Sede

Florianópolis, Brasil

Desafío

El crecimiento de la empresa la convierte en un objetivo de ciberataques, por lo que es necesario pasar de una mentalidad de empresa emergente a una cultura estratégica de seguridad.

Éxito en Cifras

- Capacitación mensual, incluida la visualización de nuevos episodios de "The Inside Man"
- Cientos de pruebas de phishing mensuales
- El porcentaje de Phish-prone (predisposición para ser víctima de phishing) en toda la organización se redujo del 20% al 3%
- La proporción entre clics y denuncias pasó de 150:10 a 6:300, lo que demuestra que los empleados mejoraron su capacidad para detectar correos electrónicos de phishing y, al mismo tiempo, informarlos al equipo de Seguridad de la Información
- Reducción global de los costos porque ya no se paga por campaña

El equipo de Seguridad de la Información contrató inicialmente a El Pescador, un proveedor de capacitación en concientización sobre seguridad con el que ya había trabajado anteriormente.

KnowBe4 Aporta Potencia y Control

El tiempo estaba del lado de Neoway. Casi inmediatamente después de incorporar a El Pescador, la organización fue adquirida por KnowBe4, lo que convirtió a Neoway en el primer cliente de KnowBe4 en Brasil.

A pesar de lo buena que había sido su experiencia con El Pescador, Costa estaba contento con la transición a la plataforma de KnowBe4.

"Nos tomamos muy en serio la concientización sobre seguridad en Neoway y necesitábamos una plataforma de capacitación en concientización sobre seguridad que nos ayudara a lograr nuestros objetivos. KnowBe4 era esa plataforma", afirma Costa. "Era muy sofisticado, personalizable y asequible; exactamente el tipo de programa que queríamos".

El programa en concientización sobre seguridad que Costa y sus colegas crearon se centraba en enseñar a los empleados la importancia de la ciberseguridad para la empresa.

"Era fundamental que nuestra fuerza laboral entendiera que proteger la empresa de las amenazas cibernéticas era importante para el éxito general de nuestro negocio y que todos debemos desempeñar un papel para lograrlo", dice Costa.

"Como teníamos tanto control sobre cómo y a quién hacíamos las pruebas con KnowBe4, aprendimos mucho sobre los hábitos de nuestros empleados".

Costa implementó un sólido programa de capacitación en concientización sobre seguridad y de phishing simulado que evaluaba a los empleados con correos electrónicos de phishing que abarcaban cuatro tipos diferentes de mensajes: aquellos de los sistemas de Neoway como Google Suite, mensajes del Departamento de RR. HH. o la gerencia, correos electrónicos de organizaciones asociadas reconocibles y temas comunes de phishing que ocurren en la práctica. También realizaron pruebas con diferentes tipos de campañas de phishing dirigidas a distintos departamentos de empleados.

"Como teníamos tanto control sobre cómo y a quién hacíamos las pruebas con KnowBe4, aprendimos mucho sobre los hábitos de nuestros empleados y lo que les tentaba a hacer clic", dice Costa. "Los correos electrónicos de phishing simulado de nuestro Departamento de RR. HH. y de nuestros sistemas internos como Google Suite fueron los que más clics generaron. Fue de gran ayuda tener una idea de lo que hacía que un empleado quisiera hacer clic".

¿Casi igual de importante? Costa se enteró de que los empleados no informaban cuando sospechaban de un correo electrónico o enlace fraudulento.

Costa continuó: "Pudimos ver que solo alrededor del 10% de los empleados utilizaban el Phish Alert Button para informar a nuestro equipo de Seguridad de la Información. Con esta información, pudimos incorporar en nuestras capacitaciones lo importante que es informar correos electrónicos sospechosos".

Tomar Decisiones Calculadas con PhishER

Con un sólido programa en concientización sobre seguridad que capacita a los empleados mensualmente y envía pruebas de phishing simulado varias veces a la semana, Costa estaba preparado para avanzar aún más.

"Les enseñamos a nuestros empleados que informar correos electrónicos sospechosos... era algo que podían hacer para mejorar la salud de nuestra organización".

"Les enseñamos a nuestros empleados que informar un correo electrónico sospechoso, ya sea un correo electrónico de phishing real o una prueba de KnowBe4 simulada, era algo que podían hacer para mejorar la salud de nuestra organización", dice Costa. "Sin embargo, con el tiempo, había ocasiones en las que teníamos 300 empleados informando algo a nuestro Departamento de Seguridad de la Información, lo cual era genial, pero también abrumador".

Fue entonces cuando Neoway incorporó **PhishER**, una plataforma ligera de orquestación, automatización y respuesta de seguridad (SOAR, Security Orchestration, Automation and Response) que gestiona el elevado volumen de mensajes potencialmente maliciosos que los usuarios informan.

Neoway y KnowBe4: Crear una Cultura de Seguridad

Según Costa, "PhishER ayuda a nuestro equipo de Seguridad de la Información a ser más prudente. Coloca los correos electrónicos informados en una cola y los prioriza para que podamos trabajar primero en los más importantes. De este modo, podemos ser más eficientes y proteger mejor a nuestra organización trabajando primero en los mensajes que suponen una mayor amenaza".

Para posicionar aún más al Departamento de Seguridad de la Información como una división comercial estratégica, Costa también presentó el **Virtual Risk Officer** (VRO) de KnowBe4 a Neoway.

"KnowBe4 nos ayudó a capacitar a nuestros empleados y a ponerlos a prueba. Luego, PhishER facilitó la notificación de amenazas y nos puso en condiciones de evaluar mejor la salud de nuestras redes frente a las amenazas de phishing", afirma Costa. "Incorporar el VRO de KnowBe4 fue un movimiento calculado para obtener una comprensión más precisa y matizada de nuestra postura ante el riesgo".

VRO proporcionó a Neoway información detallada en formato de tablero para ilustrar el riesgo que representan las personas, los departamentos, las funciones laborales y los grupos. Debido a que los empleados reciben capacitación y pruebas constantemente, sus puntajes de riesgo aumentan y disminuyen, lo que brinda a Costa y al equipo de Seguridad de la Información la oportunidad de determinar si se necesita alguna corrección en un área específica.

"Incorporar el VRO de KnowBe4 fue un movimiento calculado para obtener una comprensión más precisa y matizada de nuestra postura ante el riesgo, a fin de poder proteger aún más nuestro negocio".

Crear Conciencia, Comportamiento y Cultura

Costa implementó un cuidadoso programa de capacitación en concientización sobre seguridad. Pero, como KnowBe4 es la fuente *de facto* sobre cultura de la seguridad, complementaron este programa con otro objetivo.

"KnowBe4 nos presentó a sus expertos en cultura de la seguridad, lo que supuso un cambio radical para nosotros".

"Inicialmente, queríamos que nuestros empleados aprendieran a proteger a la organización de las amenazas de phishing, algo que KnowBe4 nos ha ayudado a conseguir; sin embargo, hemos obtenido mucho más de nuestra relación con KnowBe4", afirma Costa.

"KnowBe4 nos presentó a sus expertos en cultura de la seguridad, lo que supuso un cambio radical para nosotros. En mi opinión, Perry Carpenter de KnowBe4 es la persona más importante en seguridad de la información hoy en día porque es una autoridad en transformar la forma en que las personas perciben la seguridad, identificar sus comportamientos al respecto y comprender cómo reaccionan ante ella", comenta Costa. "Gracias a KnowBe4, cambiamos el nombre de lo que hacemos. Ya no dirigimos un programa de seguridad. Llevamos a cabo un programa de concientización, comportamiento y cultura de seguridad".

Costa sabe que una organización nunca es totalmente segura. Pero, gracias a la **plataforma de capacitación en concientización sobre seguridad y phishing simulado de KnowBe4**, PhishER y VRO, sabe que están haciendo todo lo posible para proteger los activos digitales de Neoway.

"Gracias a que KnowBe4 nos ha ayudado a entender por qué la cultura de la seguridad es tan importante, creamos una base cultural muy singular y estable que solo ayuda a nuestra organización", afirma Costa.

KnowBe4 Brazil | Av. Ibirapuera, 2315, Indianópolis, CEP 04029-200 | São Paulo-SP | Tel: +55 (0800) 761-2668 | www.KnowBe4.com | Sales@KnowBe4.com