

PHISHING ÉTICO

CASO DE ÉXITO



Echez Group, es una compañía que empodera empresas para que prosperen en un mundo digital.

Dentro de sus procesos internos, ha desarrollado un importante número de campañas de phishing ético interno, con el fin de mejorar la ciberseguridad de la organización, no solo de las amenazas externas, sino también para monitorear los riesgos internos.

TESTIMONIO → Echez Group

“ Como líder de IT en Echez Group, trabajamos constantemente para fortalecer la ciberseguridad interna y proteger nuestros activos de posibles amenazas. Para lograrlo, implementamos periódicamente una serie de campañas de phishing ético internas que nos permiten evaluar la conciencia de seguridad de nuestros empleados y detectar posibles puntos débiles en nuestra seguridad.

Gracias a estas campañas, hemos podido implementar medidas correctivas y mejorar nuestras políticas de seguridad.

Además, generamos actividades de sensibilización sobre la importancia de la seguridad de la información en toda la empresa, lo que nos ha permitido tener una cultura de seguridad más sólida en todas las áreas, reduciendo así los riesgos de posibles ataques reales. ”

Los resultados han sido muy satisfactorios, puesto que la gran mayoría de nuestros empleados demostró un comportamiento responsable, lo que refleja el impacto positivo de nuestras iniciativas.

Gracias a las campañas de phishing ético y las actividades de concientización en ciberseguridad, logramos fortalecer la seguridad de la información de nuestra empresa y garantizar un ambiente más seguro frente a las amenazas internas y externas.

Nelson Giraldo IT Leader en Echez Group

RETOS DEL PROYECTO



Identificar debilidades para descubrir posibles puntos débiles en la seguridad de la organización.



Mejorar las políticas y prácticas de seguridad.

Evaluar la conciencia de seguridad de los empleados para reconocer y reportar intentos de phishing.



Prevenir ataques reales para proteger la información confidencial y los activos de la organización.



SOLUCIONES

Con el fin de identificar y corregir las debilidades en la conciencia de seguridad de sus empleados y a su vez, mejorar la efectividad de las medidas de protección implementadas el equipo de TI de Echez Group:



Desarrolló campañas de phishing ético con las cuales se identificó la conciencia de seguridad de los empleados, abordando posibles vulnerabilidades, y mejorando las políticas y medidas de seguridad existentes.

Generó actividades de sensibilización sobre la importancia de la seguridad de la información a todos los empleados, para reconocer y responder adecuadamente a los intentos de phishing.

IMPACTO

Posterior a la realización de campañas de concientización el impacto fue:

- La identificación de los empleados que requerían mejorar sus capacidades para reconocer y reportar ataques de tipo phishing.
- El fortalecimiento de la seguridad de la información de la compañía.
- La implementación en la promoción de cultura de seguridad de la información en todas las áreas, reduciendo los riesgos de ataques reales.
- La activación de mejora en las políticas y mejores prácticas en seguridad de la información.

RESULTADOS



Al abordar las amenazas cibernéticas internas a través de pruebas realistas y éticas, la empresa pudo identificar y corregir las debilidades en la conciencia de seguridad de sus empleados.



Si bien se identificaron áreas de mejora en la conciencia de seguridad, la gran mayoría de los empleados demostraron un comportamiento responsable al no abrir ni interactuar con los correos electrónicos de phishing.

0.4% fueron usuarios comprometidos.



Aquellos que cayeron en la trampa recibieron una capacitación adicional en seguridad cibernética. 2.38% usuarios que recibieron un refuerzo en educación en ciberseguridad.



La campaña no solo logró fortalecer las defensas internas de Echez Group, sino que también promovió una cultura de seguridad cibernética entre sus empleados.

Se implementaron 11 acciones de mejora en las políticas de ciberseguridad.



Se fomentó periódicamente con el área de educación, la realización interna de los cursos de ciberseguridad.